Microsoft Exchange Server 2010 Unified Messaging

SBC Configuration Notes

Ingate SIParator

By : Microsoft

Updated : 7/24/2009

READ THIS BEFORE YOU PROCEED

1. Document Overview

Content

This document describes the configuration required to set up *Ingate SBC (SIPERATOR 19)* and *Dialogic DMG 1000 (PIMG) Gateway* using *direct SIP connectivity.* It also contains the results of the interoperability testing of Microsoft Exchange Server 2010 Unified Messaging (UM) based on this setup.

Intended Audience

This document is intended for Systems Integrators with significant telephony knowledge.

Technical Support

The information contained within this document has been provided by Microsoft partners or equipment manufacturers and is provided AS IS. This document contains information about how to modify the configuration of your SBC or VoIP gateway. Improper configuration may result in the loss of service of the SBC or gateway. Microsoft is unable to provide support or assistance with the configuration or troubleshooting of components described within. Microsoft recommends readers to engage the service of a Microsoft Exchange 2010 Unified Messaging Specialist or the manufacturers of the equipment(s) described within to assist with the planning and deployment of Exchange Unified Messaging.

Microsoft Exchange 2010 Unified Messaging (UM) Specialists

These are Systems Integrators who have attended technical training on Exchange 2010 Unified Messaging conducted by Microsoft Exchange Engineering Team. For contact information, visit here.

Version Information

Date of Modification	Details of Modification
6/22/2009	Configuration details filled in

2. Motivation and Scenario Description

2.1. Exchange Server 2010 Deployment Modes

Exchange Server 2010 can be used in two modes

1. Deployed, configured and managed on-premise by Exchange Server 2010 customers (referred to as **Exchange Server**) [*Identical to Exchange Server 2007*]
2. Deployed in a Microsoft data center and managed by Microsoft. Exchange Server 2010 customers will be able to configure Unified Messaging to suit their requirements (referred to as **Exchange Service**). [*New to Exchange Server 2010*]

2.2. Exchange Server deployment

The following figure illustrates a typical deployment at Contoso Corporation:

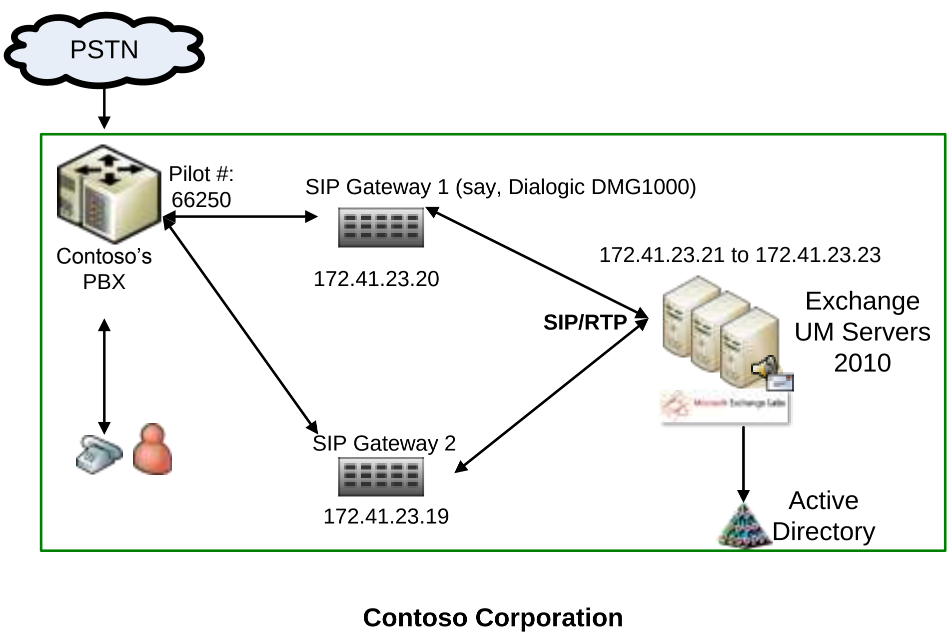


Figure 1: A typical on-premise deployment of Exchange Server 2010.

The Exchange Server Unified Messaging (UM) server roles are deployed, configured and managed by Contoso Corporation's telephony and Exchange administrators. This deployment model is identical to most Exchange Server 2007 deployments.

This document is specifically targeted towards Exchange customers interested in using the **Exchange Service** as opposed to deploying the Exchange Server themselves. The remainder of this document describes the deployment and configuration required to operate in the **Exchange Service** setting.

2.3. Exchange Service Deployment with DTAP lines per gateway

The following figure illustrates what it means for Contoso Corporation to use the Exchange Service offered from a data center deployed and managed by Microsoft. Such a deployment comes with obvious concerns as listed below the illustration.

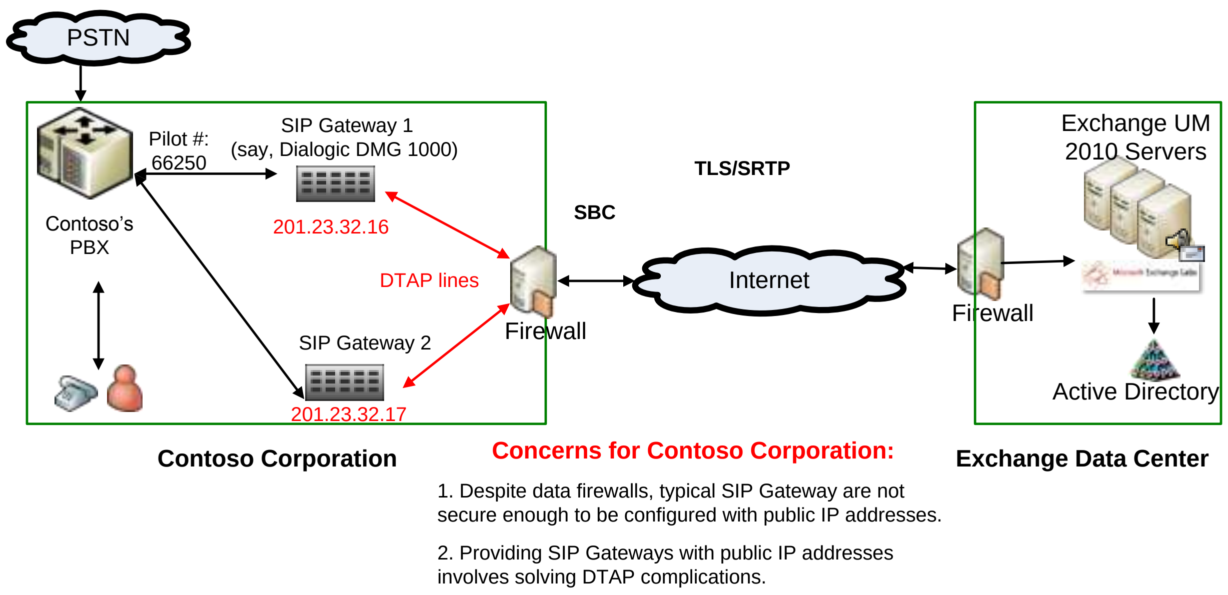


Figure 2: Contoso Corporation is using the Exchange Service via DTAP lines for its SIP Gateways.

2.4. Exchange Service Deployment with a SBC (Session Border Controller)

The concerns listed above can be alleviated with the use of a Session Border Controller. It acts as a SIP aware perimeter network element. The following figure illustrates such a deployment.

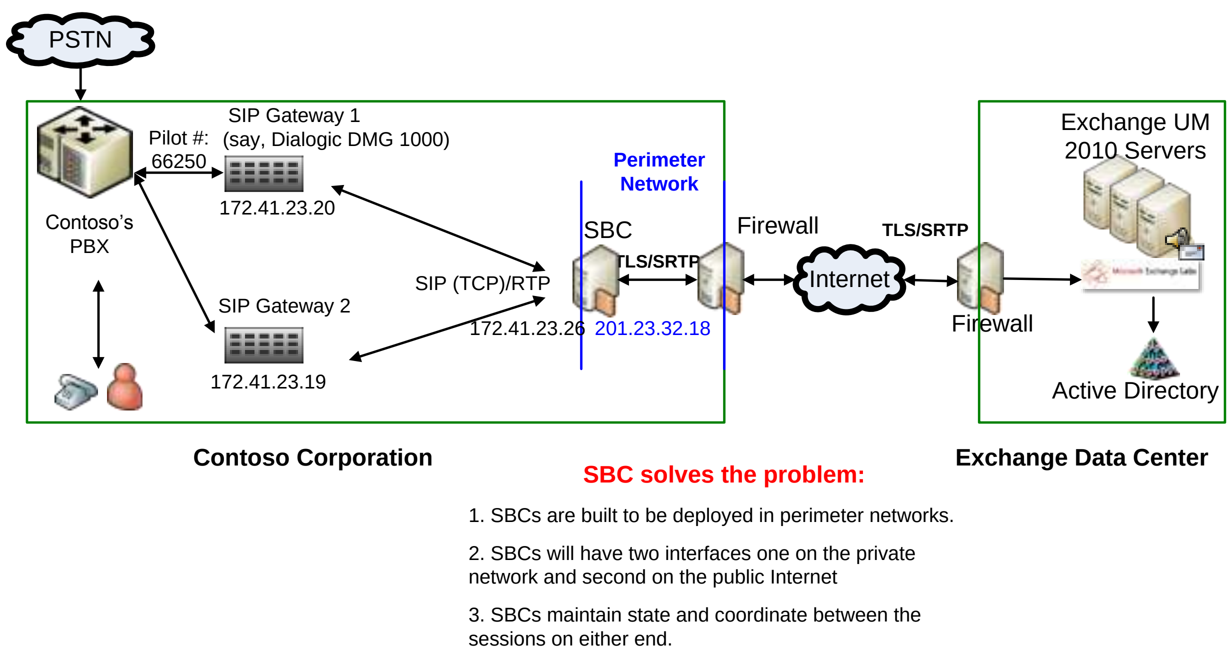


Figure 3: Contoso Corporation is using the Exchange Service via a SBC.

3. Scope of this Document

The remainder of this document provides configuration notes to achieve such a deployment. In particular, it details the configuration of the following interfaces:

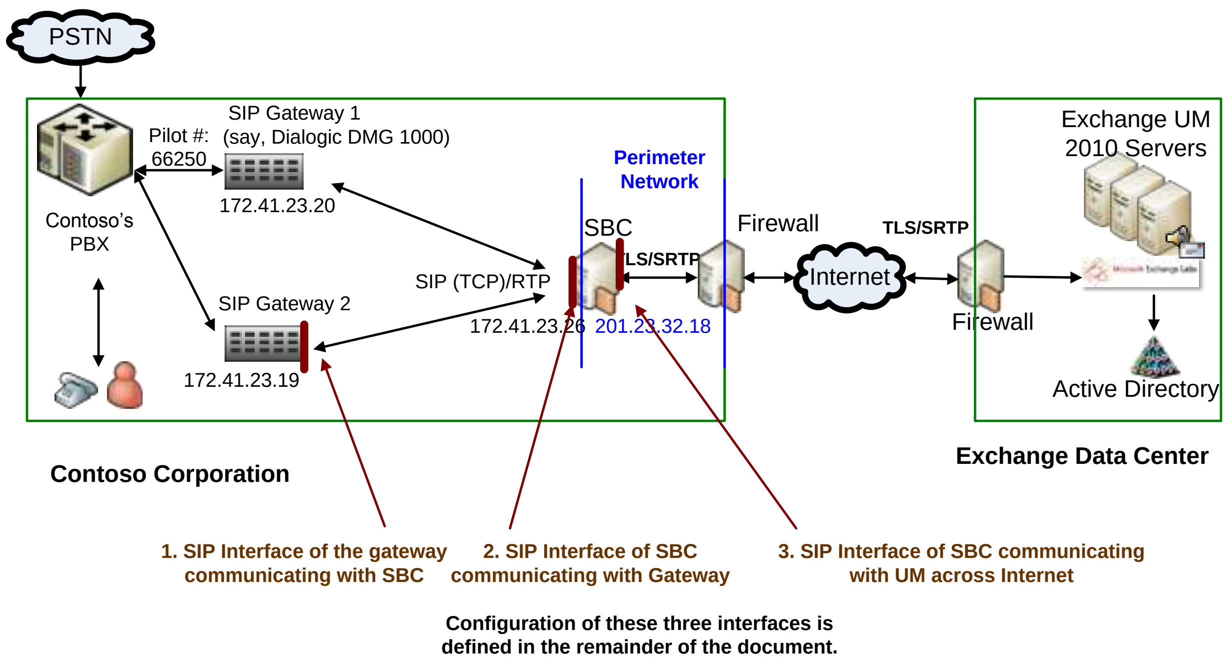


Figure 4: Interface whose configuration is described in this document.

4. Component Information

4.1. SBC

Vendor	Ingate Systems
Model	Ingate SIParator
Software	4.7.1
Additional Notes	

4.2. VoIP Gateway

Gateway Vendor	Dialogic
Model	DMG 1000
Software Version	6.0.121_74233.1
VoIP Protocol	SIP/RTP

4.3. Microsoft Exchange Server 2010 Unified Messaging

Version	14.00.611.000

5. Prerequisites

5.1. Gateway Requirements

The gateway, instead of routing all calls to Exchange UM servers, must now be configured to route all calls to SBC.

The SIP Gateway on-premise (on a private network) communicates with the private interface of the SBC using TCP and RTP. The SIP Gateway could also be configured to communicate via TLS and SRTP. However, such a configuration is beyond the scope of this documentation.

5.2. SBC Requirements

The following features must be enabled on SBC to make it ready to talk to UM and SIP Gateway:

- Enable physical interfaces
- Add network interfaces
- Add Realms and steering pools
- Enable SIP call routing and SIP Interfaces
- Create Certificate Authority (CA) and Certificate
- Upload the same CA and Certificate to SBC and UM server
- Configure SBC and UM Server for TLS

5.3. Cabling Requirements

No particular cabling requirements were identified.

6. Summary and Limitations

<This section will be filled once tests are finished>

7. Gateway Setup Notes

The gateway must be configured to receive VoIP traffic from SBC and route all VoIP traffic SBC.

7.1. VoIP Traffic Routing Setup

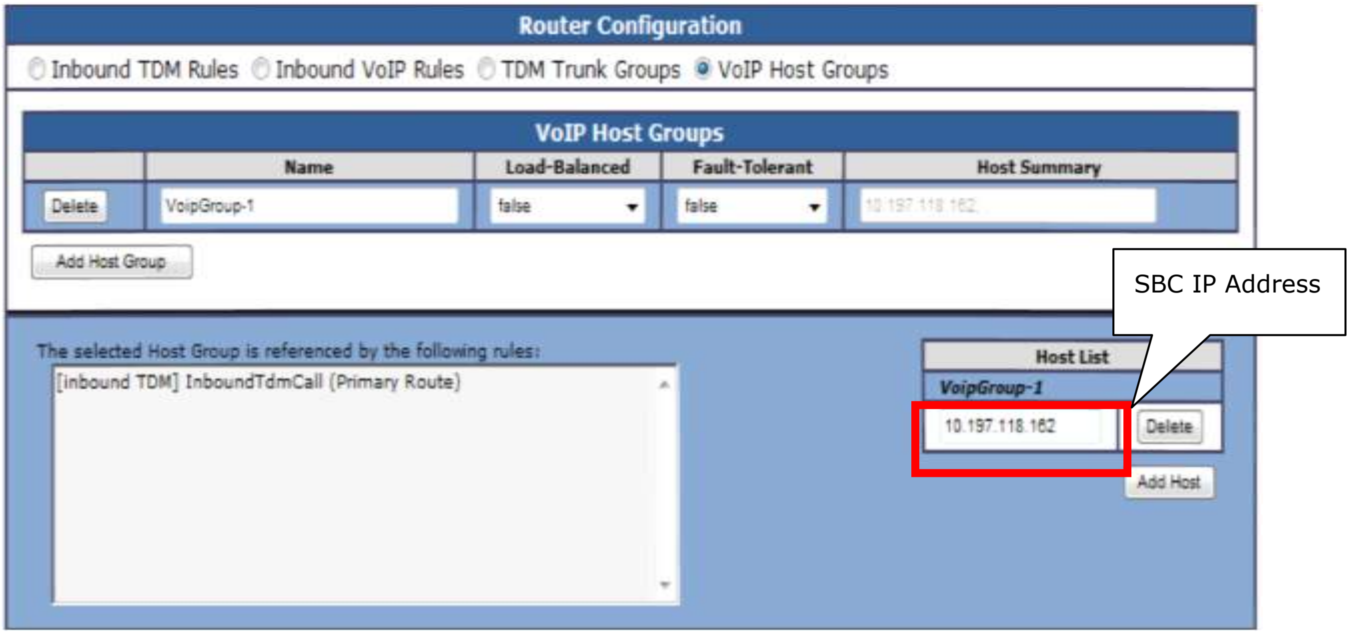


Figure 5: Gateway configuration for communicating with SBC.

7.2. TLS and Setup

As SIP Gateway will be used on-premise on the private network, TCP will be used between SBC and SIP Gateway. TLS setup will not be performed.

7.3. SRTP Setup

As SIP Gateway will be used on-premise on the private network, RTP will be used between SBC and SIP Gateway. SRTP setup will not be performed.

8. Ingate SBC Setup Notes

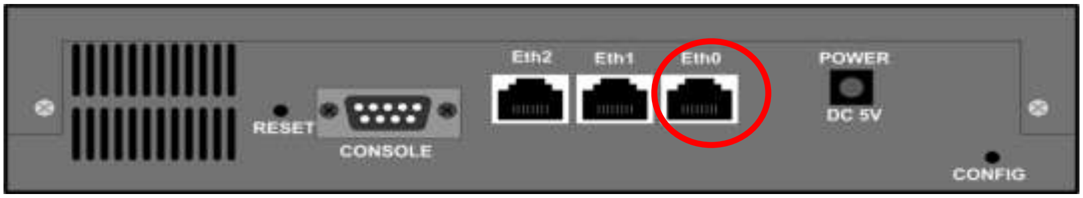
8.1. Connecting the Ingate Firewall/SIParator

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:

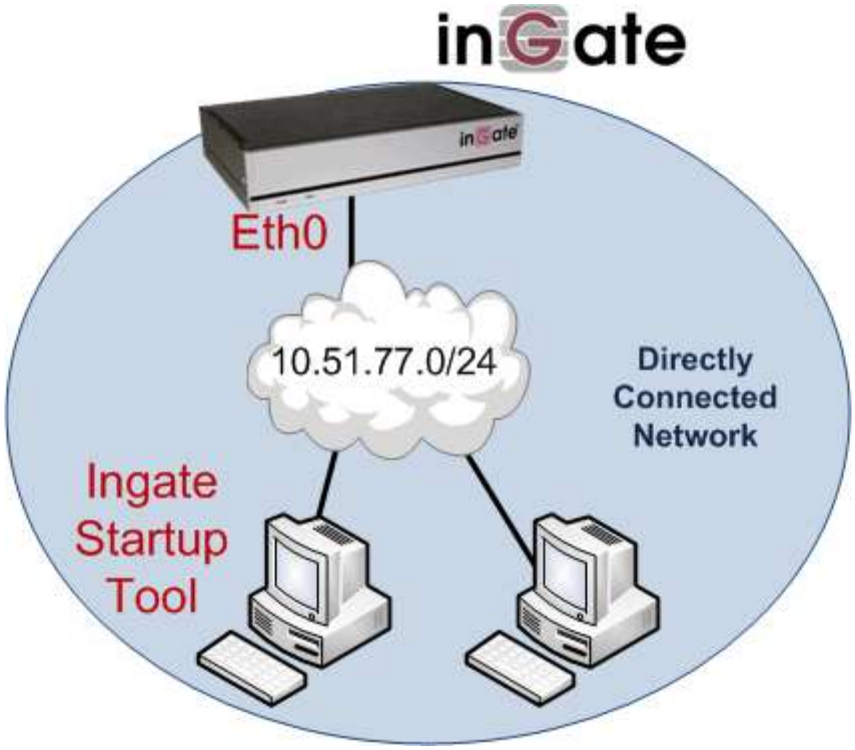
1) Connect Power to the Unit.
2) Connect an Ethernet cable to "Eth0". This Ethernet cable should connect to a LAN network. Below are some illustrations of where "Eth0" are located on SIParator



Ingate 1190 Firewall and SIParator 19 (Back)

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

8.2. Using the Startup Tool

There are two main reasons for using the Ingate Startup Tool.

- Configure the "Out of the Box" Ingate Unit for the first time.
- Change or update an existing configuration.

8.2.1. Configure the Unit for the First Time

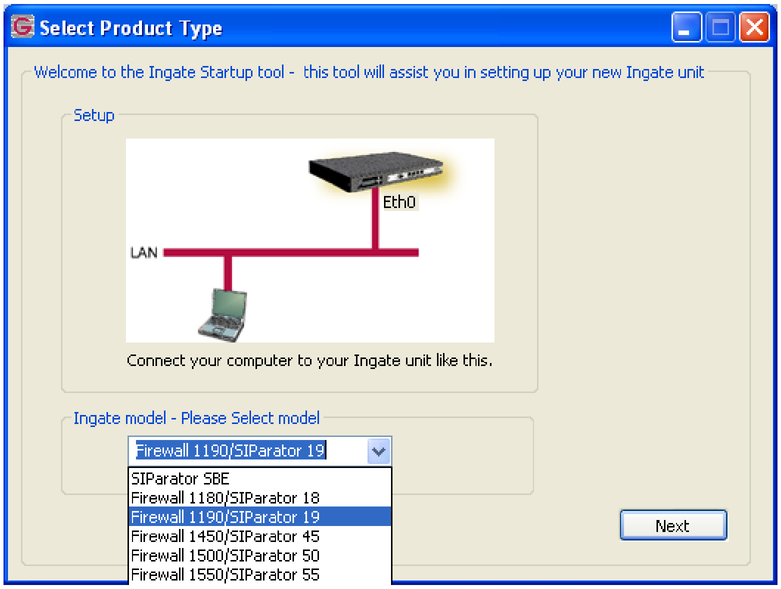
From the factory the SIParator does not come preconfigured with an IP address or Password to administer the unit. Web administration is not possible unless an IP Address and Password are assigned to the unit via the Startup Tool or Console port.

In the Startup Tool, when selecting "Configure the unit for the first time", the Startup Tool will find the Ingate Unit on the network and assign an IP Address and Password to the Ingate unit. This procedure only needs to be done ONCE. When completed, the Ingate unit will have an IP Address and Password assigned.

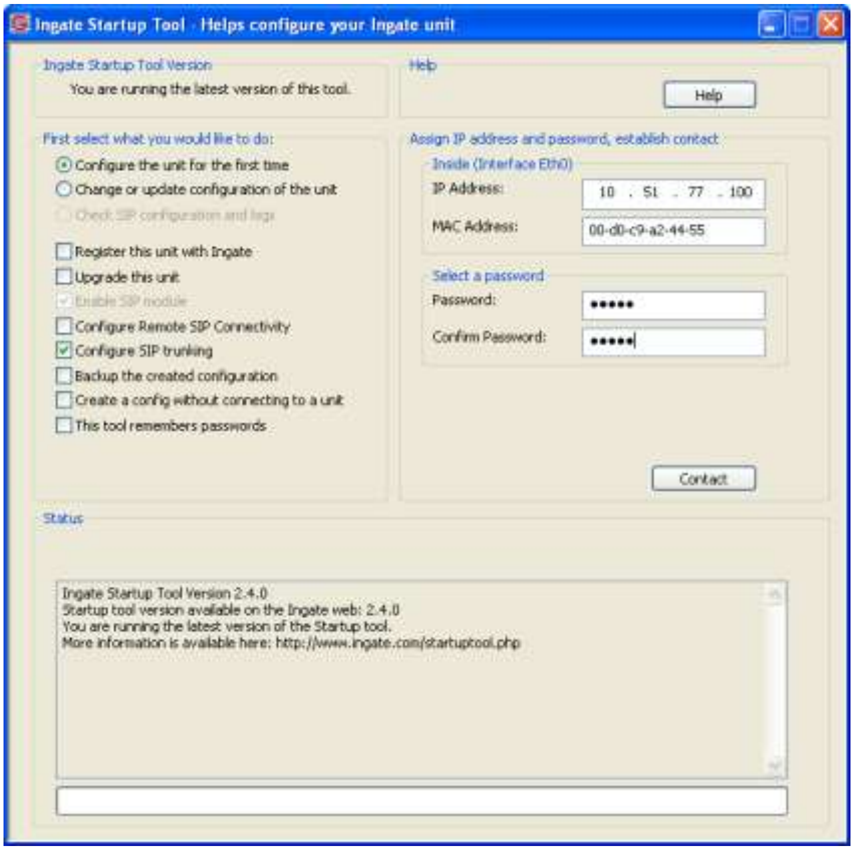
Note: If the Ingate Unit already has an IP Addressed and Password assigned to it (by the Startup Tool or Console) proceed directly to Section 8.2.2: "Change or Update Configuration".

Configuration Steps:

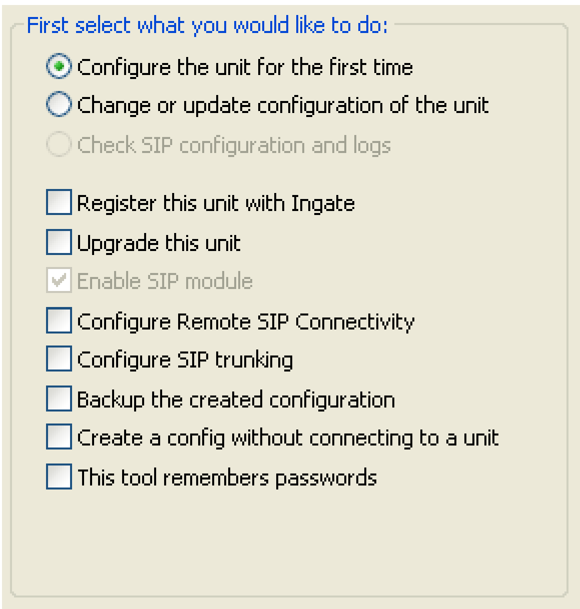
1) Launch the Startup Tool
2) Select the Model type of the Ingate Unit, and then click Next.



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



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



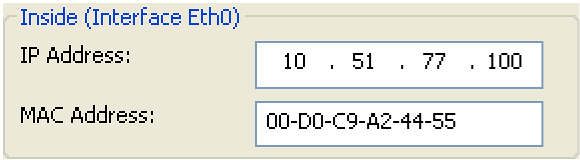
a. De-Select “Configure SIP Trunking”, as Section will discuss the manual configuration steps required to integrate with the Exchange UM Server.

b. For any other option please consult the Startup Tool – Getting Started Guide.

5) In the “Inside (Interface Eth0)”,

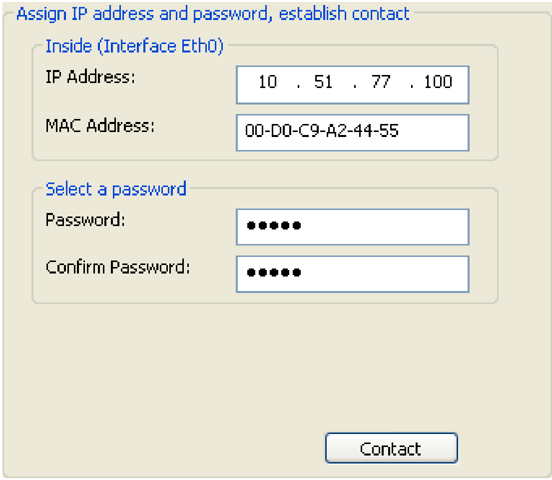
a. Enter the IP Address to be assigned to the Ingate Unit.

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 8.2.3: Network Topology.

8.2.2. Change or Update Configuration

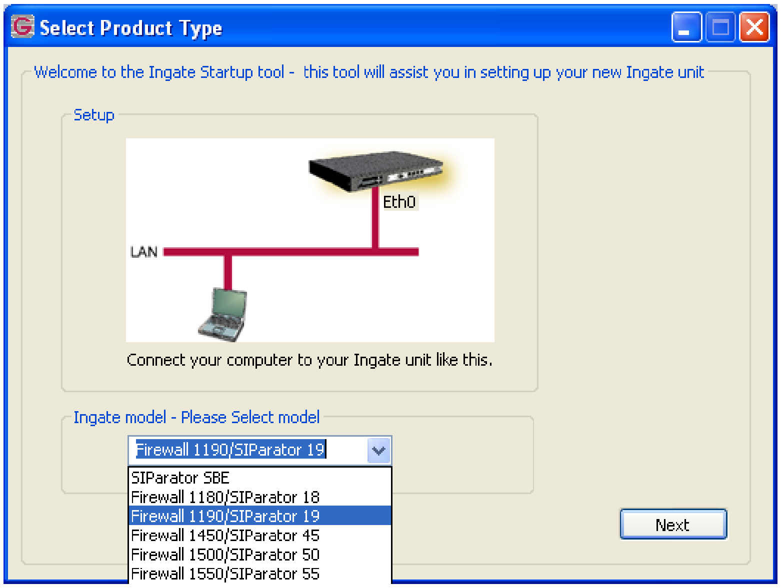
When selecting the "Change or update configuration of the unit" setting in the Startup Tool the Ingate Unit must have already been assigned an IP Address and Password, either by the Startup Tool – "Configure the unit for the first time" or via the Console port.

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

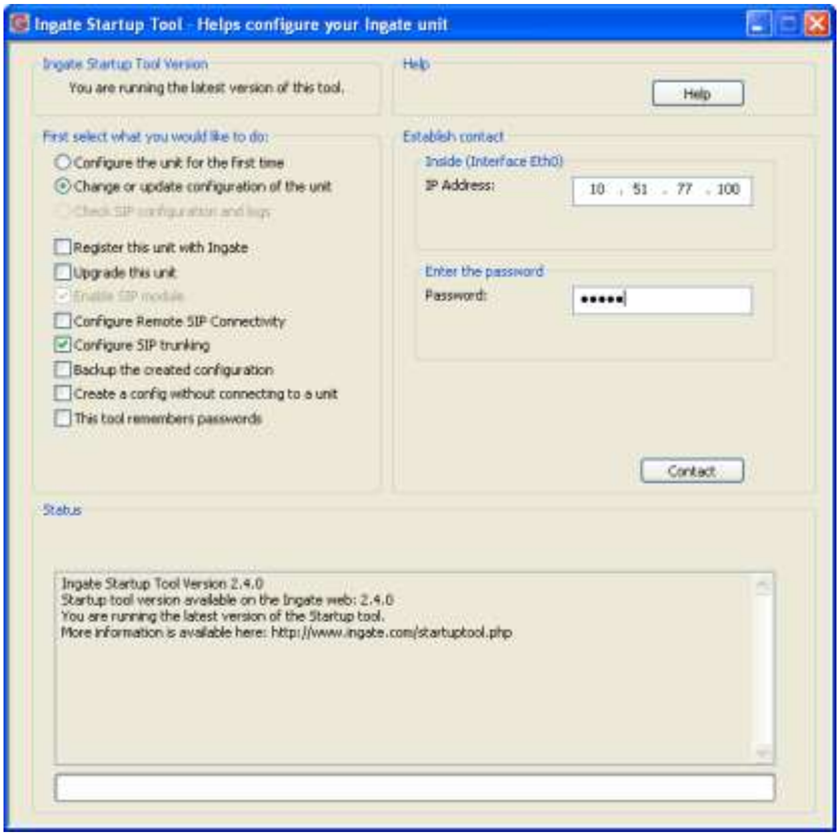
Note: If the Ingate Unit does not have an IP Addressed and Password assigned to it, proceed directly to Section 8.2.1: "Configure the Unit for the First Time".

Configuration Steps:

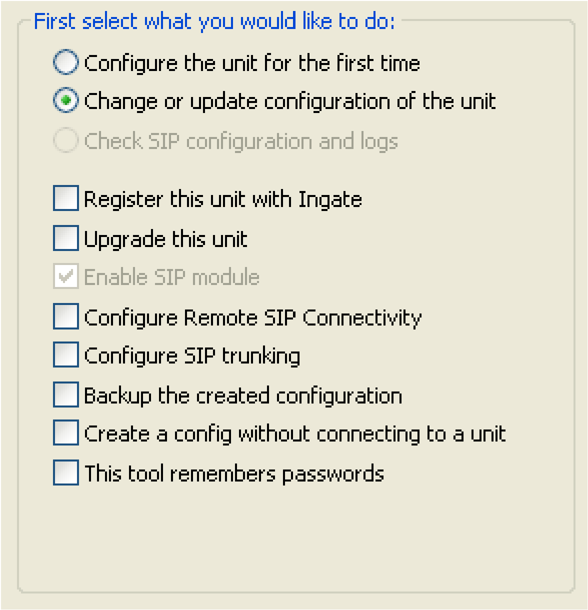
1) Launch the Startup Tool
2) Select the Model type of the Ingate Unit, and then click Next.



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



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

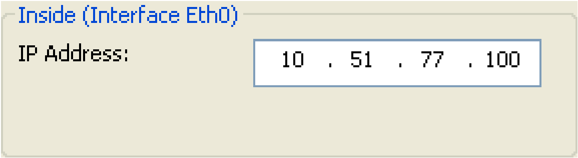


a. De-Select "Configure SIP Trunking", as Section will discuss the manual configuration steps required to integrate with the Exchange UM Server.

b. For any other option please consult the Startup Tool – Getting Started Guide.

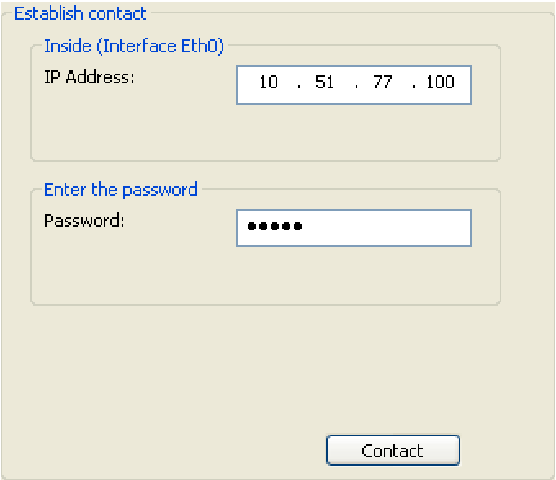
5) In the "Inside (Interface Eth0)",

a. Enter the IP Address of the Ingate Unit.



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

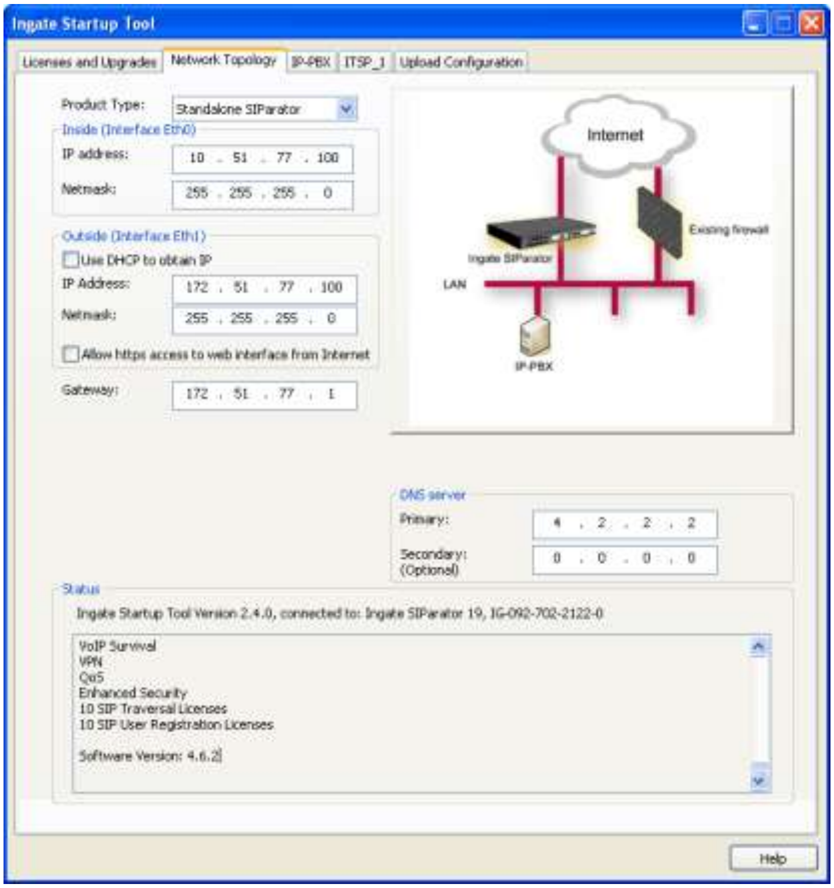
7) Once all required values are entered, the "Contact" button will become active. Press the "Contact" button to have the Startup Tool contact the Ingate unit on the network.



8) Proceed to Section 8.2.3: Network Topology.

8.2.3. Network Topology

The Network Topology is where the IP Addresses, Netmask, Default Gateways, Public IP Address of NAT'ed Firewall, and DNS Servers are assigned to the Ingate unit. The configuration of the Network Topology is dependent on the deployment (Product) type. When selected, each type has a unique set of programming and deployment requirements, be sure to pick the Product Type that matches the network setup requirements.



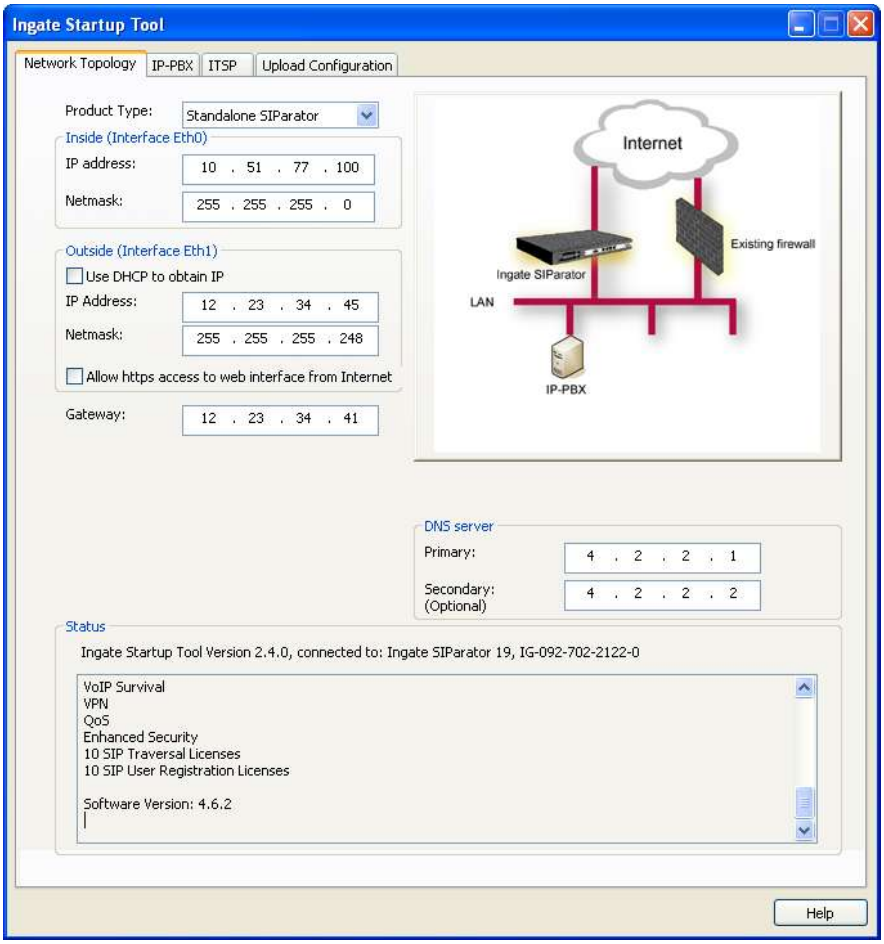
Configuration Steps:

1) In the Product Type drop down list, select Standalone SIParator.

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.

8.2.3.1 Product Type: Standalone

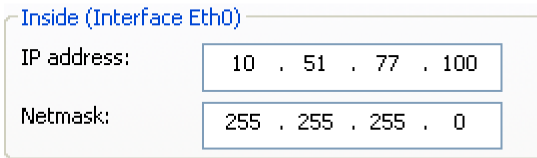
When deploying an Ingate SIParator in a Standalone configuration, the SIParator resides on a LAN network and on the WAN/Internet network. The Default Gateway for SIParator resides on the WAN/Internet network. The existing Firewall is in parallel and independent of the SIParator. Firewall is the primary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



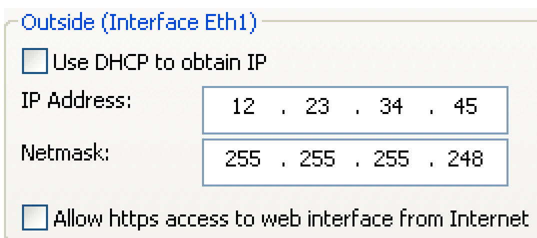
Configuration Steps:

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.

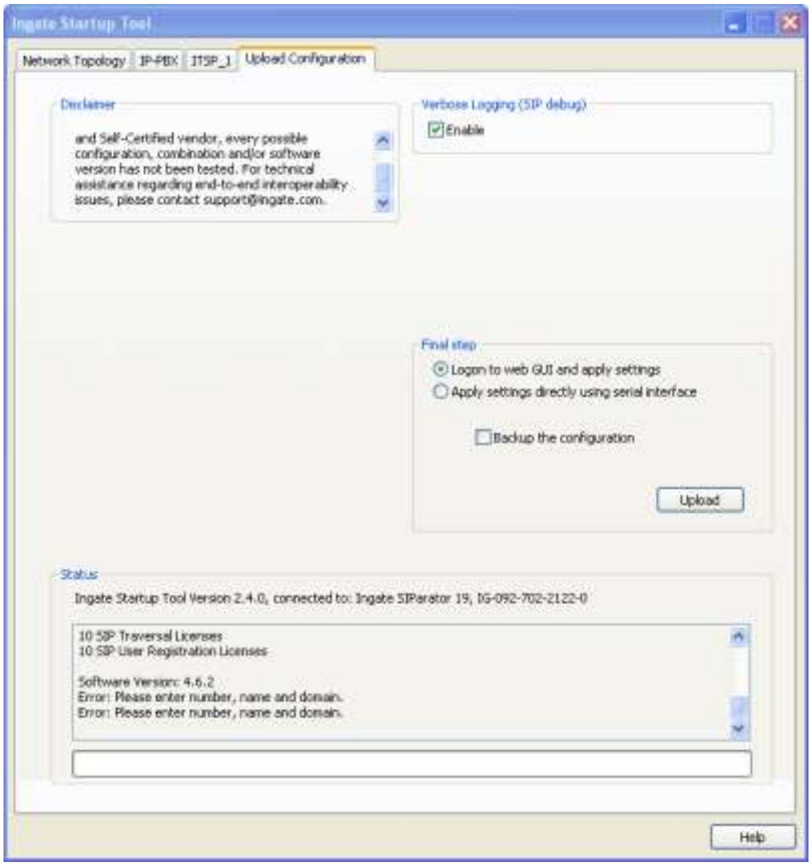


4) Enter the Default Gateway for the Ingate SIParator. The Default Gateway for the SIParator will be the existing Firewalls IP Address on the DMZ network.

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.

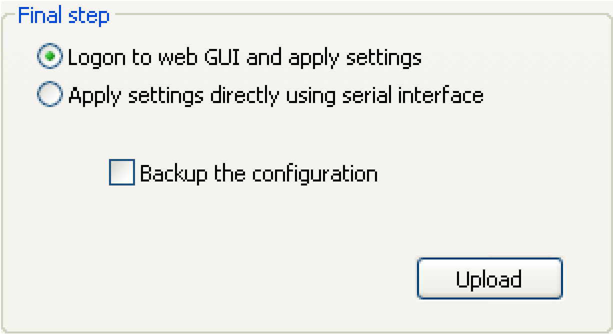
8.2.4. Upload Configuration

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.

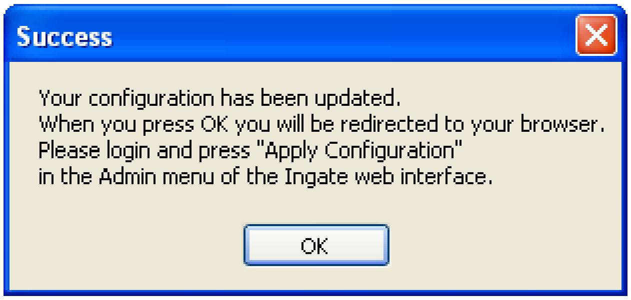


Configuration Steps:

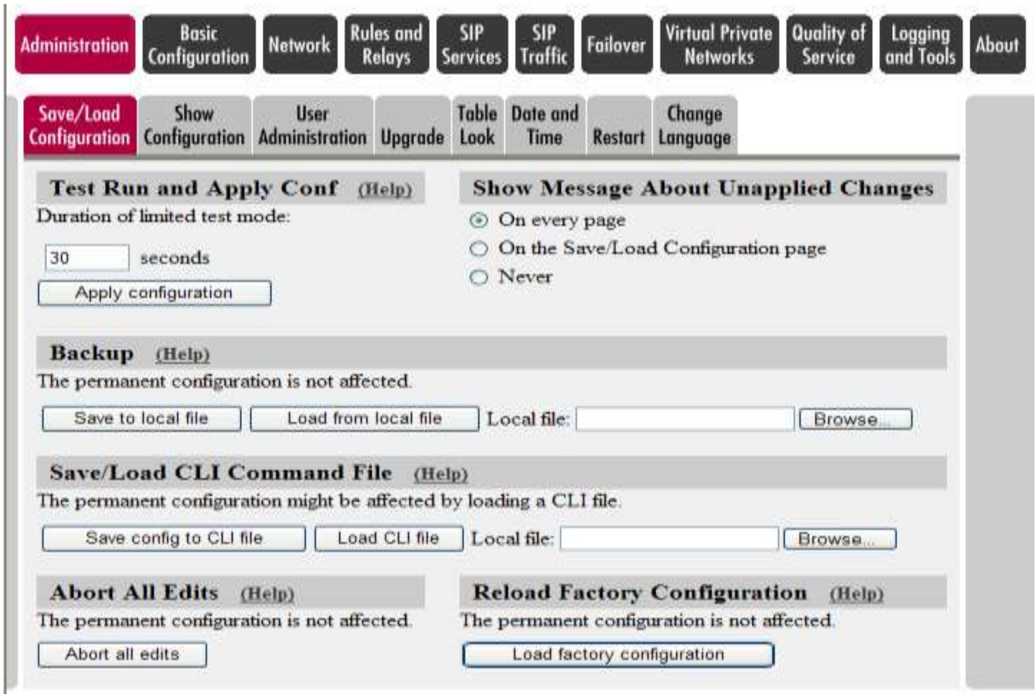
1) Press the "Upload" button. If you would like the Startup Tool to create a Backup file also select "Backup the configuration". Upon pressing the "Upload" button the Startup Tool will push a database into the Ingate unit.



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.

8.3. Network Settings

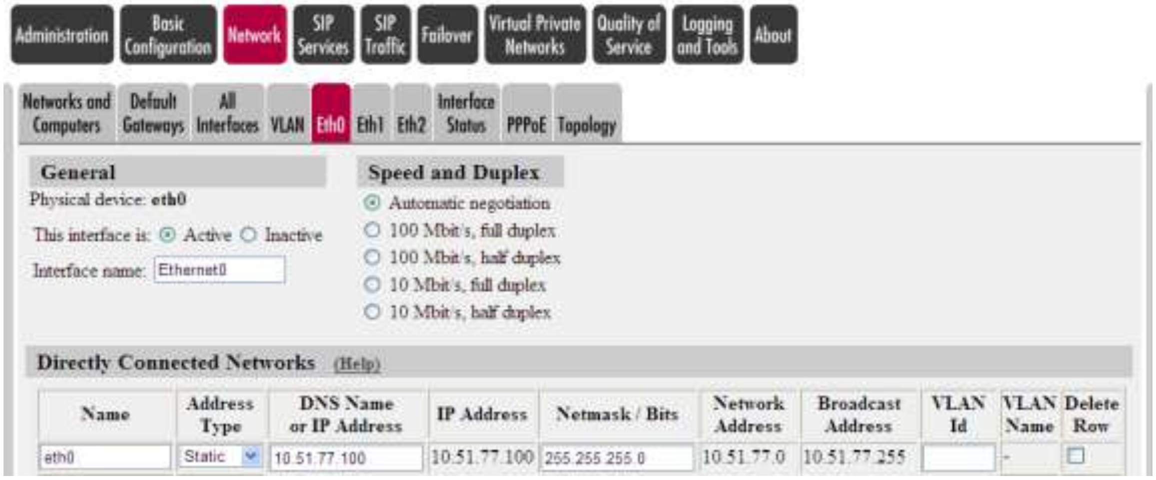
Be sure to complete Section 8.2 prior to executing this section.

Most of this configuration is configured by the Startup Tool, this is a review of the configuration.

8.3.1. Eth0 Interface

This is the LAN side interface (private network), an IP address and Mask is configured in this section.

Note: This should be completed by the Startup Tool.



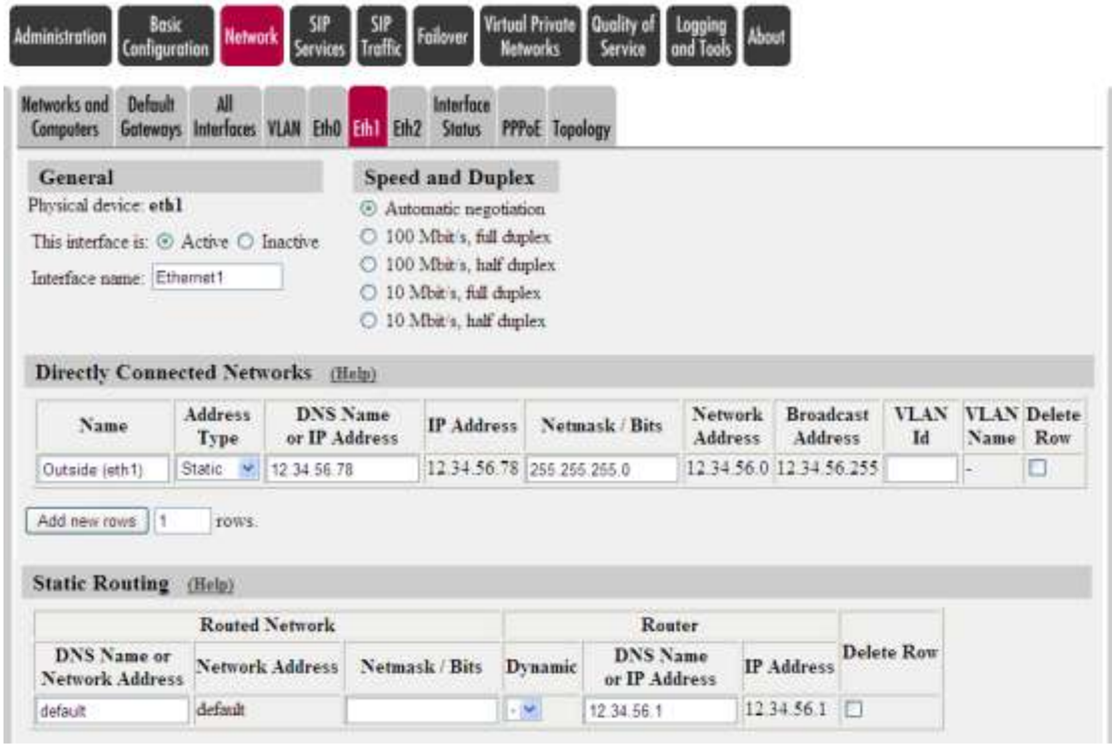
Configuration Steps

1) Under "Directly Connected Networks" add a Static IP Address for the Ingate.
2) In the "Name" field, enter a name for the interface.
3) In the "Address Type" field, select Static.
4) In the "DNS Name or IP Address" field, enter a LAN IP Address.
5) In the "Netmask/Bits" field, enter the Mask of the network

8.3.2. Eth1 Interface

This is the WAN side interface (public network), an IP address and Mask is configured in this section.

Note: This should be completed by the Startup Tool.



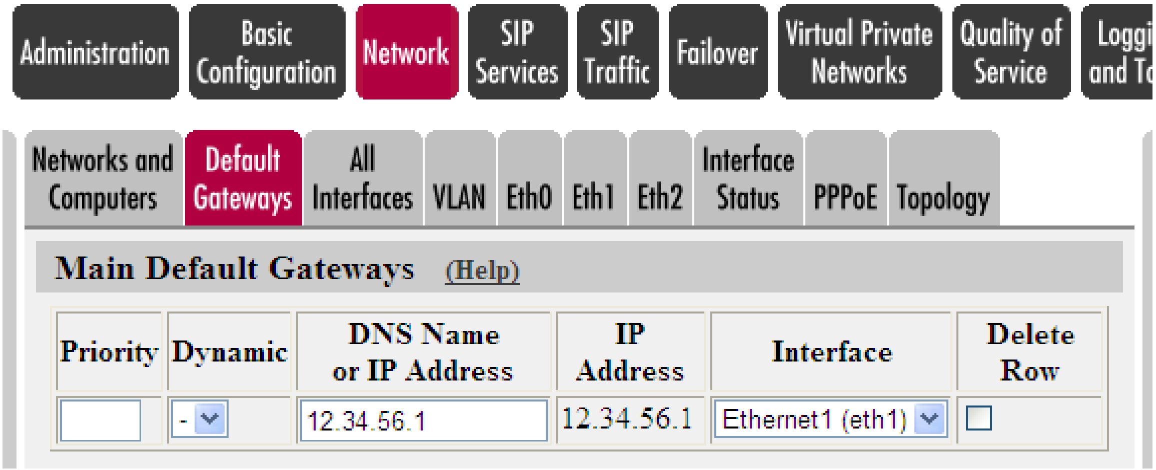
Configuration Steps

1) Under “Directly Connected Networks” add a Static IP Address for the Ingate.
   a. In the “Name” field, enter a name for the interface.
   b. In the “Address Type” field, select Static.
   c. In the “DNS Name or IP Address” field, enter a LAN IP Address.
   d. In the “Netmask/Bits” field, enter the Mask of the network
2) Under “Static Routing”, enter the default gateway
   a. In the “Routed Network” section in the “DNS Name or Network Address” field, enter “default”
   b. In the “Router” section in the “DNS Name or IP Address” field, enter the IP address of the default gateway

8.3.3. Default Gateway

This is the identification of the Default Gateway of WAN side interface (public network).

Note: This should be completed by the Startup Tool.

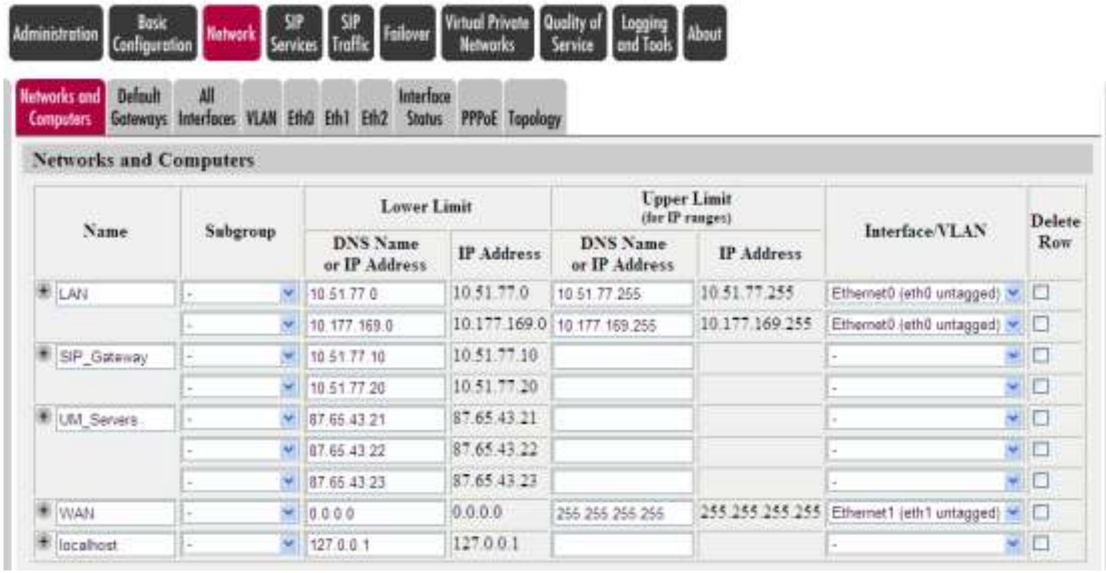


Priority	Dynamic	DNS Name or IP Address	IP Address	Interface	Delete Row
	-	12.34.56.1	12.34.56.1	Ethernet1 (eth1)	

8.3.4. Networks and Computers

This is an important section identifying locations or networks for routing purposes, and specific computers for later use in filter and traffic policies.

Note: Not all of this section is completed by the Startup Tool. Some additional requirements must be added.



Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row
		DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address		
LAN	-	10.51.77.0	10.51.77.0	10.51.77.255	10.51.77.255	Ethernet0 (eth0 untagged)	
	-	10.177.169.0	10.177.169.0	10.177.169.255	10.177.169.255	Ethernet0 (eth0 untagged)	
SIP_Gateway	-	10.51.77.10	10.51.77.10			-	
	-	10.51.77.20	10.51.77.20			-	
UM_Servers	-	87.65.43.21	87.65.43.21			-	
	-	87.65.43.22	87.65.43.22			-	
	-	87.65.43.23	87.65.43.23			-	
WAN	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	Ethernet1 (eth1 untagged)	
localhost	-	127.0.0.1	127.0.0.1			-	

Configuration Steps

1) Under “Networks and Computers” add the IP Addresses for LAN for the Ingate.
    a. In the “Name” field, enter a name for the LAN Network.
    b. Under the “Lower Limit” section, in the “DNS Name or IP Address” field enter the network address of the subnet.
    c. Under the “Upper Limit” section, in the “DNS Name or IP Address” field enter the broadcast address of the subnet.
    d. In the “Interface/VLAN” column select “Ethernet 0 (eth0 untagged)”
2) Under “Networks and Computers” add the IP Address for WAN for the Ingate.
    a. In the “Name” field, enter a name for the WAN Network.
    b. Under the “Lower Limit” section, in the “DNS Name or IP Address” field enter “0.0.0.0.
    c. Under the “Upper Limit” section, in the “DNS Name or IP Address” field enter “255.255.255.255.
    d. In the “Interface/VLAN” column select “Ethernet 1 (eth1 untagged)”
3) Under “Networks and Computers” add the IP Addresses for localhost of the Ingate.
    a. In the “Name” field, enter a name for the localhost.
    b. Under the “Lower Limit” section, in the “DNS Name or IP Address” field enter “127.0.0.1”.
    c. In the “Interface/VLAN” column select “-“
4) Under “Networks and Computers” add the IP Addresses of the SIP Gateways.
    a. In the “Name” field, enter a name for the SIP Gateways.
    b. Under the “Lower Limit” section, in the “DNS Name or IP Address” field enter the IP Address of the first SIP Gateway.
    c. If there are more than one SIP Gateway, click the (+) button to add another entry to the same group, and under the “Lower Limit” section, in the “DNS Name or IP Address” field enter the IP Address of the next SIP Gateway.
    d. In the “Interface/VLAN” column select “-”
5) Under “Networks and Computers” add the IP Addresses of the Exchange UM.
    a. In the “Name” field, enter a name for the SIP Gateways.
    b. Under the “Lower Limit” section, in the “DNS Name or IP Address” field enter the IP Address of the first Exchange UM Server.
    c. If there are more than one SIP Gateway, click the (+) button to add another entry to the same group, and under the “Lower Limit” section, in the “DNS Name or IP Address” field enter the IP Address of the next Exchange UM Server.
    d. In the “Interface/VLAN” column select “-”

8.3.5. Basic Configuration – DNS Servers

DNS Servers are essential to the operation of the UM Server. They need to be able to resolve all of the Fully Qualified Domain Names of the Exchange UM Servers.

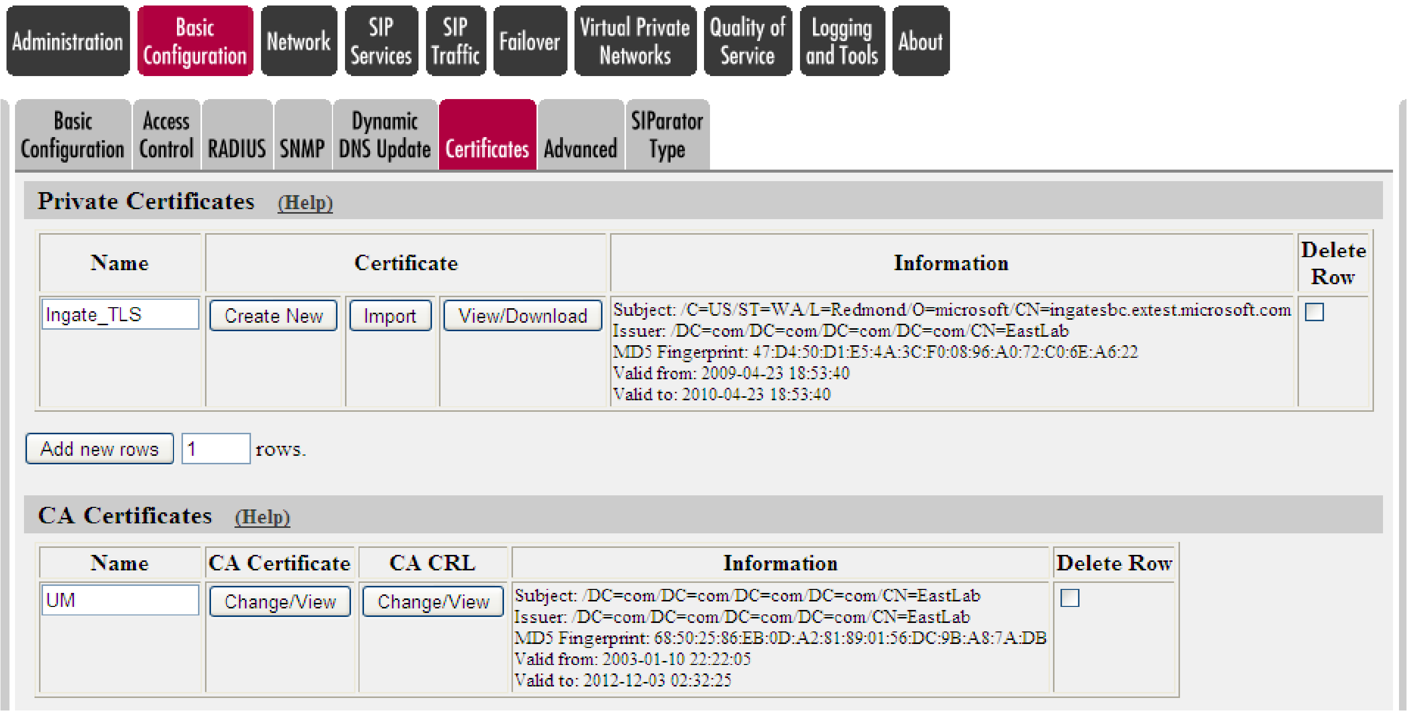
Note: This should be completed by the Startup Tool.

8.4. SIP Signaling Encryption

This section is for setting up TLS Transport in preparation for Encrypted SIP communications between the Ingate and Exchange UM.

8.4.1. Certificates

TLS Transport is about certificate exchange, on Peer having a unique Certificate to share with the other Peer, with each having a copy of the others Certificate. The Ingate Certificate to provide the UM Server is generated as a Private Certificate. The UM Servers Certificate given to the Ingate is imported as a CA Certificate.



8.4.1.1 Private Certificate

The Private Certificate is the Certificate that is used by SIParator and is provided to Exchange UM Server by SIParator during TLS negotiation. Generate a certificate request which will be submitted to CA to generate a certificate.

Configuration Steps:

Create certificate request

1) In the "Create Certificate" section enter data in the following fields;
   a. In the "Expire in (days), enter the number of days the certificate is valid for.
   b. In the "Country Code (C)" field, enter "US" for USA
   c. In the "Organization (O) field, enter the company name.
   d. In the "Common Name (CN) field, enter the Administrators name.
   e. In the "State/Province" field, enter the State or Province your are in.
   f. In the "Organizational Unit" field, enter the department you are in.
   g. In the "Email Address: field, enter the Administrators email address.
   h. In the "Location/Town (L), enter the City you are in.
   i. In the "Serial Number" field, enter any number 1 or higher.
   j. Press "Create an X.509 Certificate request".
   k. Press "View/Download"
   l. Press "download certificate\certificate request in PEM format" and save in a file.
   m. Pass this certificate request to CA to generate a certificate.

Import a Certificate

1) Press "Import"

2) Brows the certificate (PKCS12 (.p12) or PEM (.pem) format) generated from CA for Ingate SIParator.
3) Press “Import signed certificate”.

8.4.1.2 CA Certificate

The CA Certificate belongs to the Certificate Authority, which signed the private certificate. The Ingate SIParator uses this certificate for validation of trusted certificates.

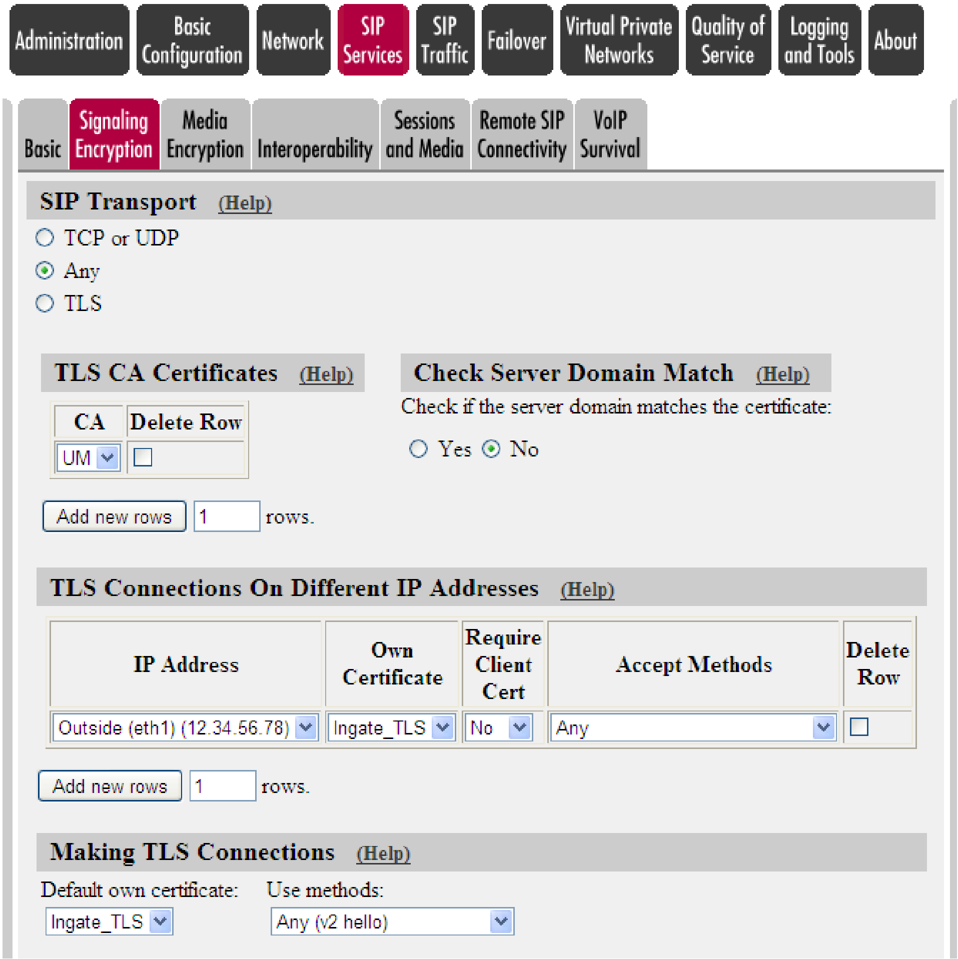
Configuration Steps:

Import a Certificate

1) Browse to a file in a PKCS12 (.p12) or PEM (.pem) format certificate.
2) Press the “Import CA Certificate” button.

8.4.2. Signaling Encryption (TLS Setup)

In SIP Services -Signaling Encryption section is the definition of the Certificate exchange between the Ingate and the Exchange UM.



Configuration Steps:

1) Under "SIP Transport", select "Any"
2) Under "TLS CA Certificates", select the CA Certificate create earlier.
3) Under "Check Server Domain Match", select "No"
4) Under "TLS Connections on Different IP Addresses" select the following:
    a. Under the "IP Address" column, select the WAN Interface (IP Address).
    b. Under the "Own Certificate" column, select the Private Certificate uploaded earlier.
    c. Under the "Require Client Cert" column, select "No".
    d. Under the "Accept Methods" column, select "Any".
5) Under the "Making TLS Connections"
    a. For the "Default own certificate, select the Private Certificate uploaded earlier
    b. For the "Use methods", select "Any (v2 hello)

8.5. SIP Traffic (General)

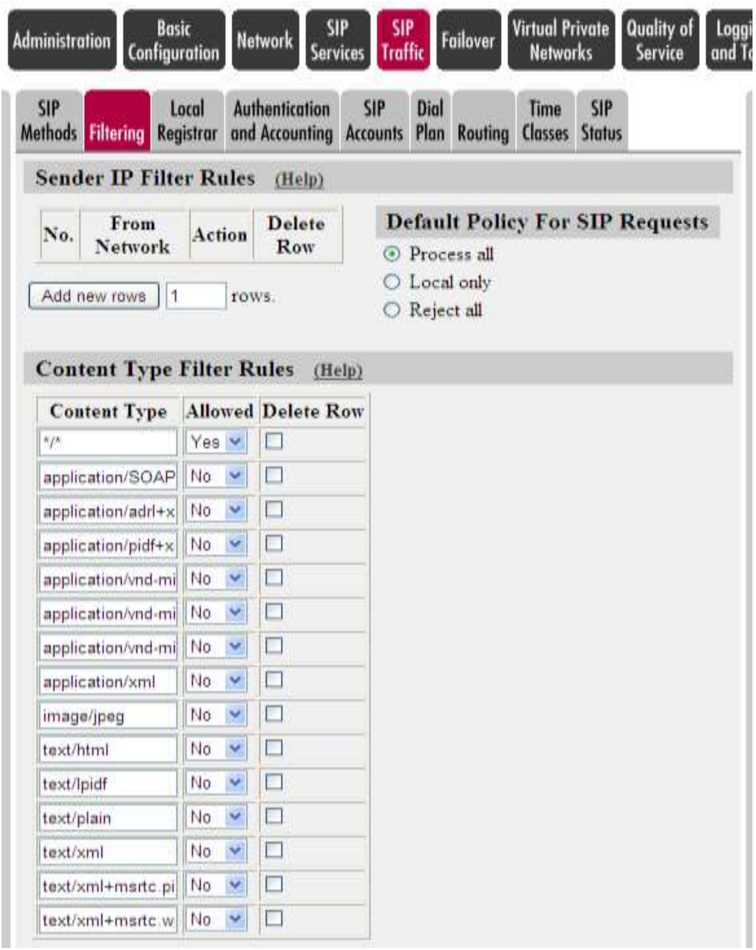
These are some general SIP Traffic Rules and Policies that need to be in place for general operation.

Note: This should be completed by the Startup Tool.

8.5.1. Filtering

For Sender IP Filter Rules, you set all the rules for SIP requests from different networks. Requests that do not match any rule are handled according to the Default Policy For SIP Requests.

For Content Type Filter Rules, the SIParator will only let through SIP packets that have one of the content types (MIME types) listed below. Please note that SIP packets with the content types "application/sdp", "application/xpidf+xml" and "text/x-msmsgsinvite" are always forwarded, as well as SIP packets with no body at all.



Configuration Steps:

1) Under "Content Type Filter Rules,
   a. For the "Content Type" column, enter " */* " for allow all MIME Content.
   b. For the "Allowed" column, select "Yes"

8.6. Call Flow from the SIP Gateway to Exchange UM

Here we define the Dial Plan and SIP Domain Routing for SIP Gateway calls to be routed to the Exchange UM Servers. There are direct calls for IVR usage and Domain forwards for Mailbox usage.

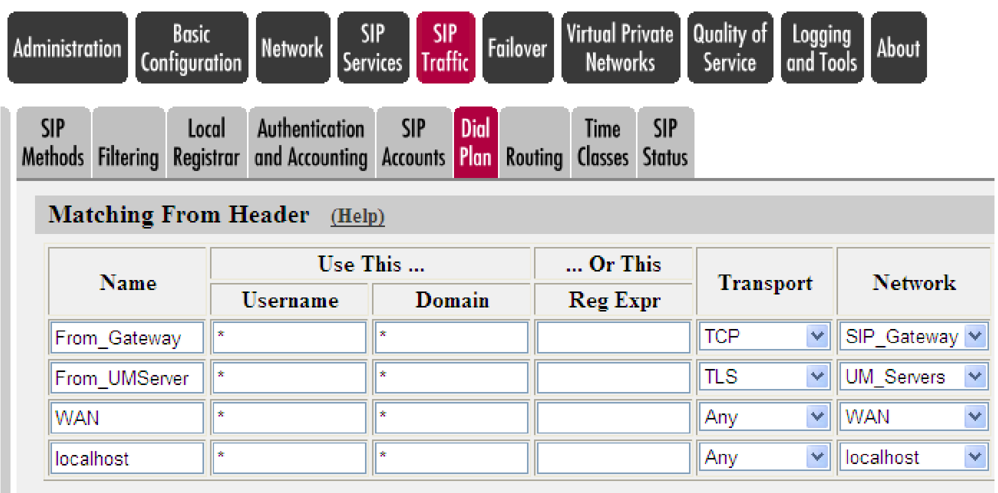
8.6.1. Dial Plan

The Dial Plan is an advanced routing tool for SIP signaling. For each line in the Dial Plan, you can match an incoming SIP message on the SIP From header and the Request-URI. Based on this, you will be able to define how the SIP message should be forwarded. The Dial Plan can be turned On or Off.

8.6.1.1. Matching From Header

Here you create criterias for the From header of the SIP messages. This is used when matching requests in the Dial Plan. For a request to match, all criterias must be fulfilled. In the Username and Domain columns, you can use "*", meaning any username/domain.

The criteria here will be to match calls coming from the SIP Gateways.



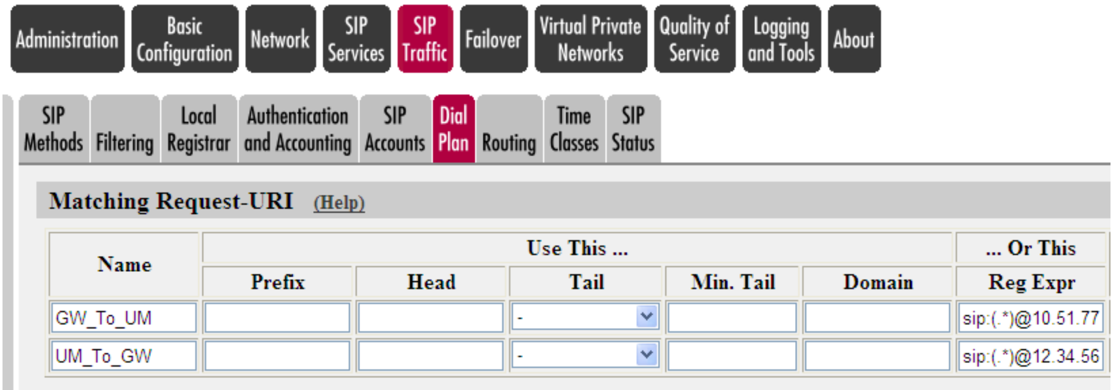
Configuration Steps:

1) Create an entry for the SIP Gateways
    a. Under the “Name” column, enter any name to identify the entry.
    b. In the “Use This …” section, under the “Username” column, enter a “ * ”.
    c. In the “Use This …” section, under the “Domain” column, enter a “ * ”.
    d. Under the “Transport” column, select the Transport be used by the SIP Gateway.
    e. Under the “Network” column, select the Network created in “Networks & Computers” that identified the IP Addresses of the SIP Gateways.
2) Create an entry for the LocalHost
    a. Under the “Name” column, enter any name to identify the entry.
    b. In the “Use This …” section, under the “Username” column, enter a “ * ”.
    c. In the “Use This …” section, under the “Domain” column, enter a “ * ”.
    d. Under the “Transport” column, select “ANY”.
    e. Under the “Network” column, select the Network created in “Networks & Computers” that identified the IP Address of the LocalHost.
3) Create an entry for the WAN
    a. Under the “Name” column, enter any name to identify the entry.
    b. In the “Use This …” section, under the “Username” column, enter a “ * ”.
    c. In the “Use This …” section, under the “Domain” column, enter a “ * ”.
    d. Under the “Transport” column, select “ANY”.
    e. Under the “Network” column, select the Network created in “Networks & Computers” that identified the IP Addresses of the WAN.

8.6.1.2 Matching Request URI

Here you create criterias for the Request-URI of the SIP messages. This is used when matching requests in the Dial Plan. For a request to match, all criterias must be fulfilled.

The criteria here will be to match calls coming from the SIP Gateways. The SIP Gateways will be sending INVITEs directly to the Ingate IP Address. For Example: 65432@10.51.77.100, thus the Ingate needs to look for “Any number @ 10.51.77.100”.



Configuration Steps:

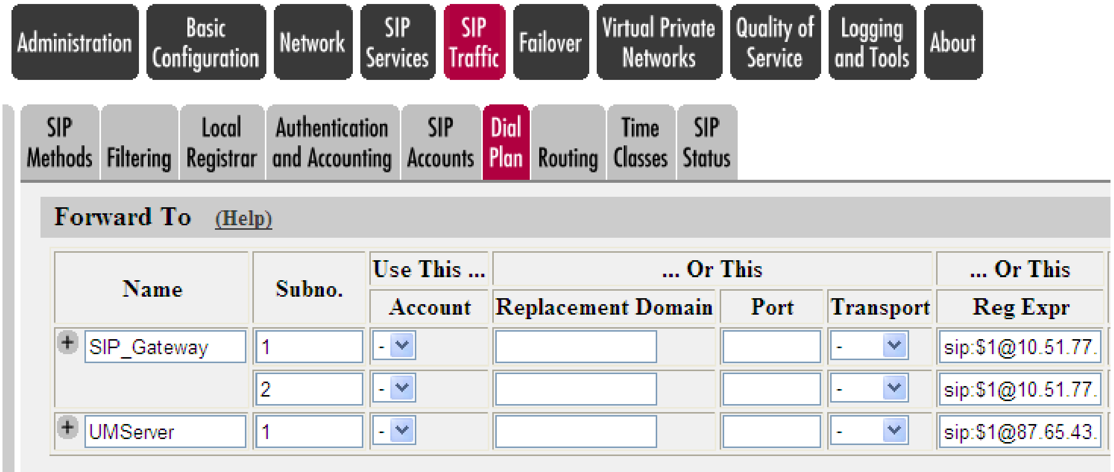
1) Create an entry to match the Request URI Header being sent from the SIP Gateway to the Ingate
    a. Under the "Name" column, enter any name to identify the entry.
    b. In the "… Or This" section, under the "Reg Expr" column, enter the following Regular Expression; "sip:(.*)@LAN_IP_Address_of_Ingate"
    c. In the "Use This …" section, under the "Tail" column, select " – ".

8.6.1.3 Forward To

Here you may define where and how the SIParator should forward the request using the Dial Plan. Expressions can be defined either by selecting an account from the SIP Accounts table, or by defining a replacement URI, port and transport.

You can also define a regular expression that refers to Reg Exp subexpressions on the corresponding row in the Matching Request-URI table. Subexpressions are numbered in the order of their starting paranthesis and referred to as $number. In the expression (sip:(.+))@ingate.com, which matches any Request-URI like sip:user@ingate.com, there are two referable subexpressions: sip:user, which is referred to as $1, and user, which is referred to as $2. You can always refer to the entire Request-URI with $0, as long as the match in the Matching Request-URI table was made using a Reg Exp.

The criteria here will be to define the Exchange UM servers for the calls coming from the SIP Gateways to be forwarded to. Also here is the definition of the TLS Transport and Port for TLS. For example sip:$1@87.65.43.21:5061;transport=TLS



Configuration Steps:

1) Create an entry for the Exchange UM Server,
   a. Under the "Name" column, enter any name to identify the entry.
   b. In the "… Or This" section, under the "Reg Expr" column, enter the following Regular Expression; "sip:$1@WAN_IP_Address_of_ExchangeUM:5061;transport=TLS"

8.6.1.4 Dial Plan

For each line, select a From entry and Request-URI to match. Then select an Action and, optionally, a Forward to entry to define how the matching requests should be handled by the SIParator.

Here is where all of the previous criteria are put together to define the call flow. Calls from the SIP Gateways calling the Ingate IP Address are to be forwarded to the Exchange UM Server over TLS.

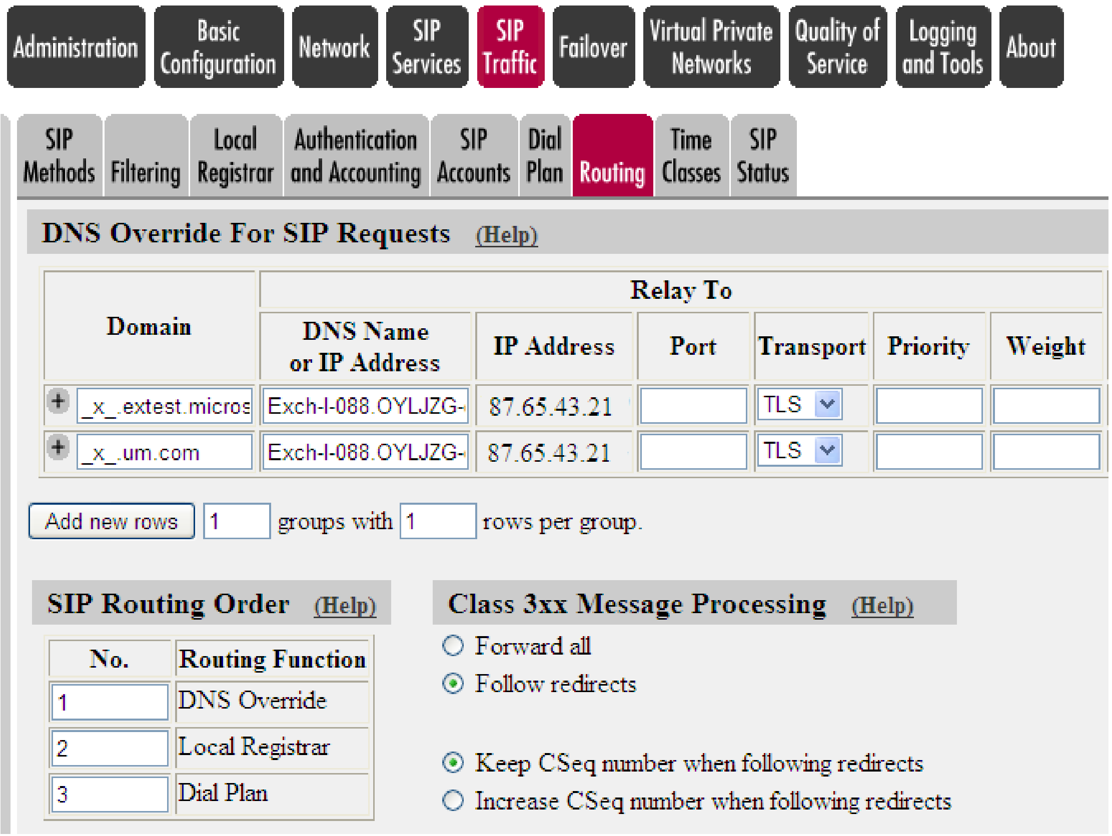
Configuration Steps:

1) Create an entry for that defines the call flow,
    a. Under the “From Header” column, select the “Matching From Header” criteria entered earlier for calls coming from the SIP Gateways.
    b. Under the “Request URI” column, select the “Matching Request URI” criteria entered earlier for calls coming to the Ingate LAN IP.
    c. Under the “Action” column, select “Forward”.
    d. Under the “Forward To” column, select the “Forward To” criteria entered earlier that defines the location of the Exchange UM.
2) Create an entry for that defines the localhost,
    a. Under the “From Header” column, select the “Matching From Header” criteria entered earlier for calls coming from the LocalHost.
    b. Under the “Request URI” column, select the “Matching Request URI” enter “-“.
    c. Under the “Action” column, select “Allow”.
    d. Under the “Forward To” column, select the “Forward To” enter “-“.

8.6.2. DNS Override for SIP Requests

Here, you enter SIP domains not handled by the SIParator and which cannot be looked up using DNS. Note that the Request-URI will not be rewritten when this setting is used. It will only cause the SIParator to send the SIP request to the new destination.

“ _*_ ” is used to identify a Wildcard Domain Name. The Exchange UM Servers use various wildcard domains with an Exchange Forest. This setting allows the Ingate to route the various domains to appropriate UM Servers.



Configuration Steps:

1) Under "DNS Override for SIP Requests":
    a. In the "Domain" column, enter the wildcard with domain on the Exchange UM Server.
    b. Under the "Relay To" section, under the "DNS Name or IP Address", enter the Exchange UM servers DNS Host name or IP Address.
    c. Under the "Relay To" section, under the "Transport", select "TLS" as the transport.
2) Under "Class 3XX Message Processing"
    a. Select "Follow redirects"
    b. Select "Keep CSeq number when following redirects"

8.7. Call Flow from Exchange UM to SIP Gateway

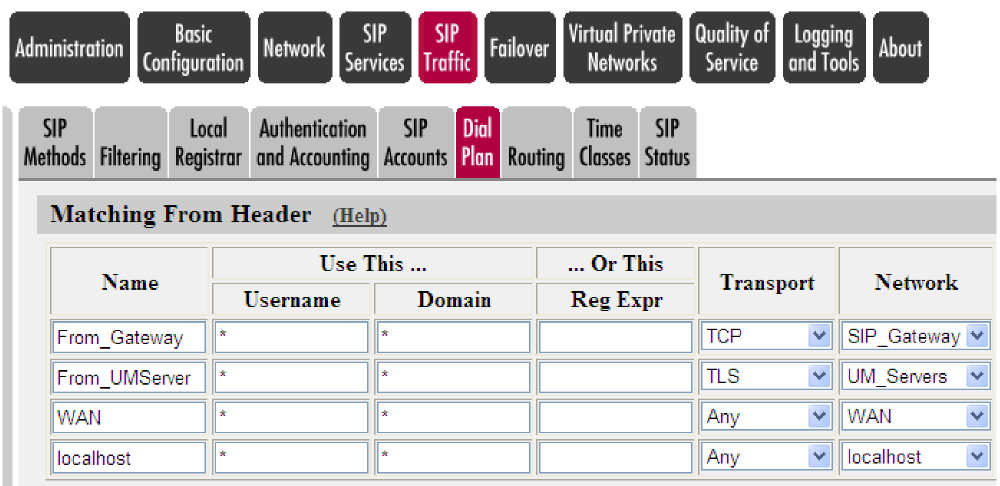
Here we define the Dial Plan for Exchange UM Server calls to be routed to the SIP Gateways. These are calls in the opposite direction then described in the previous section. There are direct calls from various outdialing applications within the Exchange UM.

8.7.1. Dial Plan

The Dial Plan is an advanced routing tool for SIP signaling. For each line in the Dial Plan, you can match an incoming SIP message on the SIP From header and the Request-URI. Based on this, you will be able to define how the SIP message should be forwarded. The Dial Plan can be turned On or Off.

Here you create criteria's for the From header of the SIP messages. This is used when matching requests in the Dial Plan. For a request to match, all criterias must be fulfilled. In the Username and Domain columns, you can use "*", meaning any username/domain.

The criteria here will be to match calls coming from the Exchange UM.



Name	Use This ...		... Or This	Transport	Network
	Username	Domain	Reg Expr		
From_Gateway	*	*		TCP	SIP_Gateway
From_UMServer	*	*		TLS	UM_Servers
WAN	*	*		Any	WAN
localhost	*	*		Any	localhost

Configuration Steps:

1) Create an entry for the Exchange UM
    a. Under the "Name" column, enter any name to identify the entry.
    b. In the "Use This …" section, under the "Username" column, enter a " * ".
    c. In the "Use This …" section, under the "Domain" column, enter a " * ".
    d. Under the "Transport" column, select "TLS".
    e. Under the "Network" column, select the Network created in "Networks & Computers" that identified the IP Addresses of the Exchange UM.
2) Create an entry for the LocalHost

    Note: (same as section 4.4.1.1)

    a. Under the "Name" column, enter any name to identify the entry.
    b. In the "Use This …" section, under the "Username" column, enter a " * ".
    c. In the "Use This …" section, under the "Domain" column, enter a " * ".

d. Under the “Transport” column, select “ANY”.
e. Under the “Network” column, select the Network created in “Networks & Computers” that identified the IP Address of the LocalHost.

3) Create an entry for the WAN

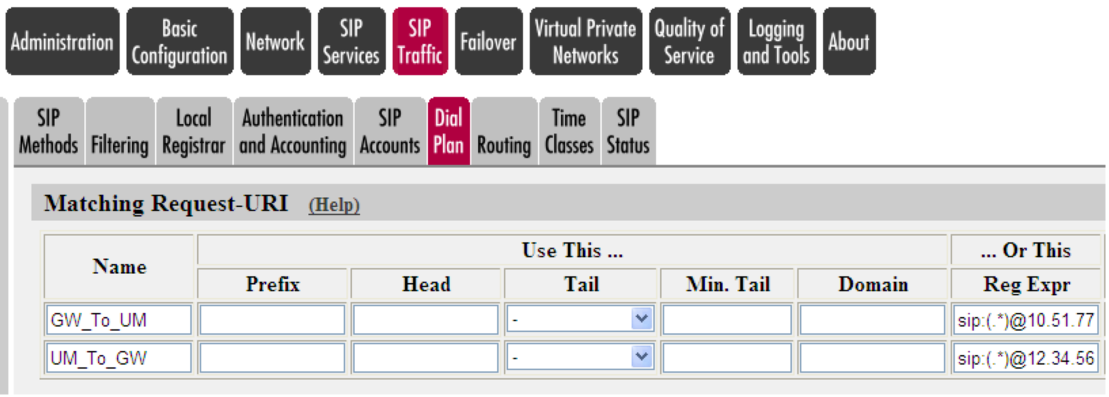
Note: (same as section 4.4.1.1)

a. Under the “Name” column, enter any name to identify the entry.
b. In the “Use This …” section, under the “Username” column, enter a “ * ”.
c. In the “Use This …” section, under the “Domain” column, enter a “ * ”.
d. Under the “Transport” column, select “ANY”.
e. Under the “Network” column, select the Network created in “Networks & Computers” that identified the IP Addresses of the WAN.

8.7.1.1 Matching Request URI

Here you create criterias for the Request-URI of the SIP messages. This is used when matching requests in the Dial Plan. For a request to match, all criterias must be fulfilled.

The criteria here will be to match calls coming from the Exchange UM. The Exchange UM will be sending INVITEs directly to the Ingate WAN IP Address. For Example: 6139630933@12.34.56.78, thus the Ingate needs to look for “Any number @ 12.34.56.78”.



Configuration Steps:

1) Create an entry to match the Request URI Header being sent from the Exchange UM to the Ingate

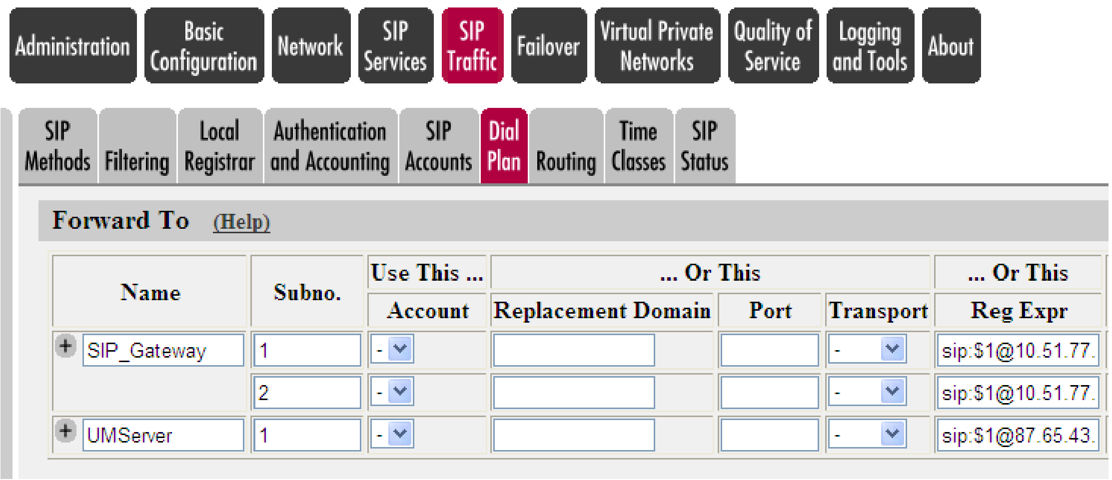
a. Under the “Name” column, enter any name to identify the entry.
b. In the “… Or This” section, under the “Reg Expr” column, enter the following Regular Expression; “sip:(.*)@WAN_IP_Address_of_Ingate”
c. In the “Use This …” section, under the “Tail” column, select “ – “.

8.7.1.2 Forward To

Here you may define where and how the SIParator should forward the request using the Dial Plan. Expressions can be defined either by selecting an account from the SIP Accounts table, or by defining a replacement URI, port and transport.

You can also define a regular expression that refers to Reg Exp subexpressions on the corresponding row in the Matching Request-URI table. Subexpressions are numbered in the order of their starting paranthesis and referred to as $number. In the expression (sip:(.+))@ingate.com, which matches any Request-URI like sip:user@ingate.com, there are two referable subexpressions: sip:user, which is referred to as $1, and user, which is referred to as $2. You can always refer to the entire Request-URI with $0, as long as the match in the Matching Request-URI table was made using a Reg Exp.

The criteria here will be to define the SIP Gateways for the calls coming from the Exchange UM to be forwarded to. Also here is the definition of the TLS Transport and Port for TLS. For example sip:$1@10.51.77.10:5060;transport=TCP



Configuration Steps:

1) Create an entry for the SIP Gateways,
    a. Under the "Name" column, enter any name to identify the entry.
    b. In the "… Or This" section, under the "Reg Expr" column, enter the following Regular Expression; "sip:$1@LAN_IP_Address_of_SIP_Gateways:5060;transport=TCP"
2) If there is more than one SIP Gateway,
    a. Press the (+) button to create a secondary contactable SIP gateway
    b. In the "… Or This" section, under the "Reg Expr" column, enter the following Regular Expression; "sip:$1@LAN_IP_Address_of_SIP_Gateways:5060;transport=TCP"

8.7.1.3 Dial Plan

For each line, select a From entry and Request-URI to match. Then select an Action and, optionally, a Forward to entry to define how the matching requests should be handled by the SIParator.

Here is where all of the previous criteria are put together to define the call flow. Calls from the Exchange UM calling the Ingate WAN IP Address are to be forwarded to the SIP Gateways over TCP.

Configuration Steps:

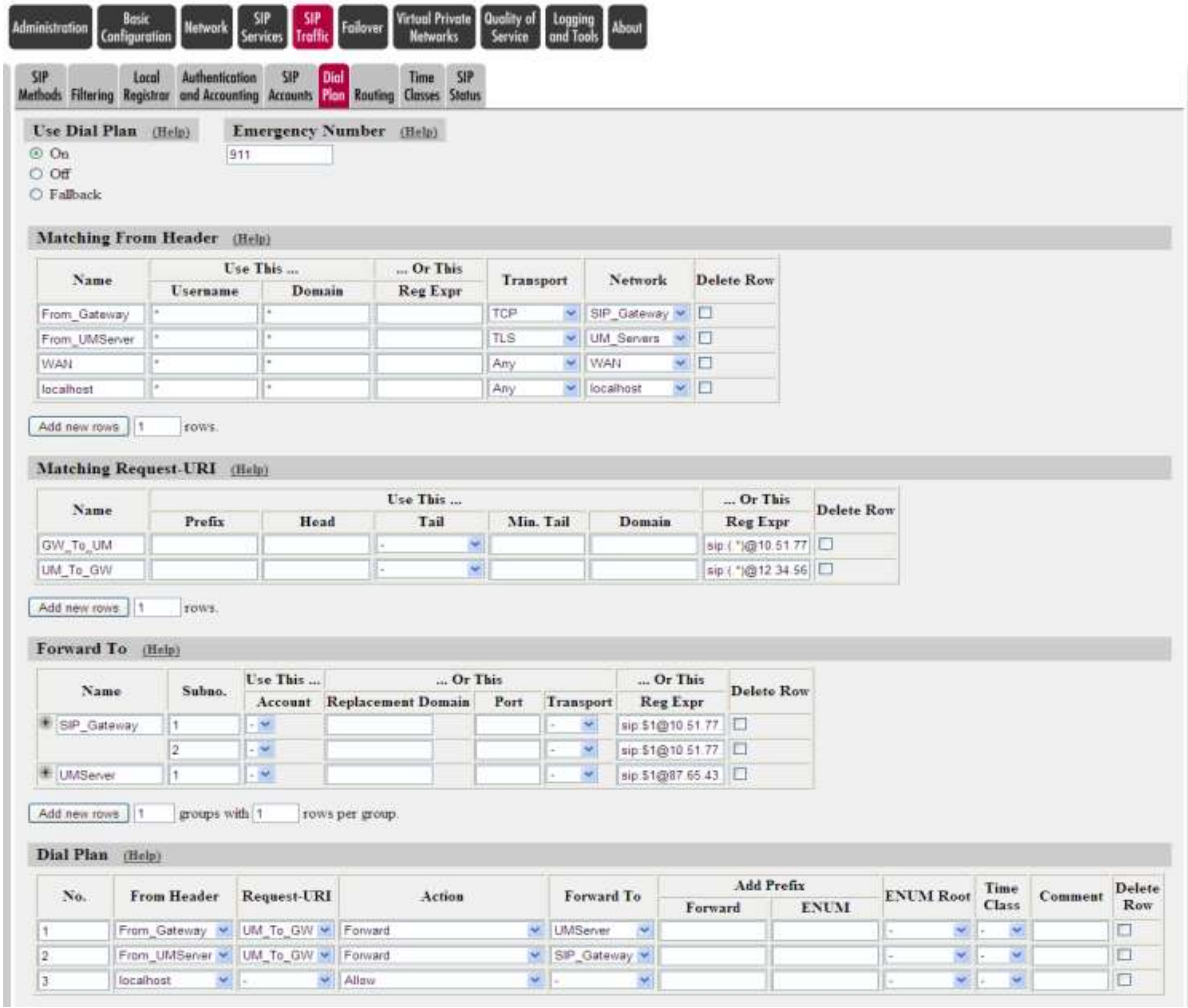
1) Create an entry for that defines the call flow,
    a. Under the "From Header" column, select the "Matching From Header" criteria entered earlier for calls coming from the Exchange UM.
    b. Under the "Request URI" column, select the "Matching Request URI" criteria entered earlier for calls coming to the Ingate WAN IP.
    c. Under the "Action" column, select "Forward".
    d. Under the "Forward To" column, select the "Forward To" criteria entered earlier that defines the location of the SIP Gateway.
2) Create an entry for that defines the localhost,

   Note: (same as section 4.4.1.4)
    a. Under the "From Header" column, select the "Matching From Header" criteria entered earlier for calls coming from the LocalHost.
    b. Under the "Request URI" column, select the "Matching Request URI" enter "-".
    c. Under the "Action" column, select "Allow".
    d. Under the "Forward To" column, select the "Forward To" enter "-".

8.8. Overview of Dial Plan

Here is the complete Dial Plan, the three criteria, “Matching From Header”, “Matching Request URI” and “Forward To”. Then the call flow is defined in the “Dial Plan” section.

The “Dial Plan” in conjunction with the “DNS Override for SIP Requests”, provide all of the routing definition in the Ingate to define the call flow and Transport requirements.



8.9. Fail-Over Configuration

This information will be provided later as required.

9. Exchange 2010 UM Validation Test Matrix

The following table contains a set of tests for assessing the functionality of the UM core feature set with SBC. The results are recorded as either:

- Pass (**P**)
- Conditional Pass (**CP**)
- Fail (**F**)
- Not Tested (**NT**)
- Not Applicable (**NA**)

Refer to:

- Appendix for a more detailed description of how to perform each call scenario.
- Section 6.1 for detailed descriptions of call scenario failures, if any.

Testing Scenarios

No.	**Call Scenarios (see appendix for more detailed instructions)**	(**P**/**CP**/**F**/**NT**/**NA**)	**Reason for Failure (see 6.1 for more detailed descriptions)**
1	**Call Establishing** Dial the pilot number from a phone extension that is not enabled for Unified Messaging and logon to a user's mailbox. And make sure that call is established Confirm hearing the prompt: "Welcome, you are connected to Microsoft Exchange. To access your mailbox, enter your extension…"		
2	**Call Answering** Test different scenarios of call answering 2.1 Call is answered by the user. 2.2 There is a message from UM and then leave a voice mail.		

	2.3 Tests for Fax Message.		
3	**Subscriber Access** Retrieve Voice mail, email, contacts and calendar information from mailbox of an individual user.		
4	Dial user extension and leave a voicemail		
4a	Dial user extension and leave a voicemail from an internal extension. Confirm the Active Directory name of the calling party is displayed in the sender field of the voicemail message.		
4b	Dial user extension and leave a voicemail from an external phone. Confirm the correct phone number of the calling party is displayed in the sender field of the voicemail message.		
5	Dial Auto Attendant (AA). Dial the extension for the AA and confirm the AA answers the call.		
6	Test **Call Transfer** by Directory Search.		
6a	Call Transfer by Directory Search and have the called party answer. Confirm the correct called party answers the phone.		
6b	Call Transfer by Directory Search when the called party's phone is busy.		

	Confirm the call is routed to the called party's voicemail.		
6c	Call Transfer by Directory Search when the called party does not answer. Confirm the call is routed to the called party's voicemail.		
6d	Setup an invalid extension number for a particular user. Call Transfer by Directory Search to this user. Confirm the number is reported as invalid.		
7	Outlook Web Access (OWA) **Play-On-Phone Feature.**		
7a	Listen to voicemail using OWA's Play-On-Phone feature to a user's extension.		
7b	Listen to voicemail using OWA's Play-On-Phone feature to an external number.		
8	Test **Call routing** across forest Call is routed from one forest to other forest.		
9	Test **Message Waiting Indicator** (MWI). On receiving voice message notifies the user about receiving a message Geomant offers a third party solution: MWI 2010. Installation files and product documentation can be found on Geomant's MWI 2007 website.		
10	Test **MWI-SMS**		

	Confirm SMS.		
11	Load Balancing		
12	Security Testing		
13	Performance/Stress testing		
14	Monitoring through SNMP(Admin Monitoring)		

9.1. Security Testing Scenarios

	Type of attack	Brief description	(P/CP/F/NT/NA)	Reason for Failure
1	**TCP SYN attack**	Client sends a SYN, gets a SYN-ACK, but never sends the ACK		
2	**TCP connection attack**	Client makes many connections using socket-level resources on the Server. However, no meaningful data is ever sent.		
3	**TLS negotiation attack**	Unauthorized client makes many simultaneous TLS connections to server and makes the server do expensive TLS negotiation for up to 32 seconds prior to disconnection.		
2	**TLS connection attack**	Client makes many TLS connections, however, no data is ever sent.		
3	**Unused connections**	Client creates many connections and initially sends data, but later		

		sends no data on, tying up server resources and preventing it from servicing other meaningful requests.		
4	**Unauthenticated connections**	In the absence of a pre-configured authorized list at the connection level, unauthorized client can make the server do expensive I/O prior to call being denied.		
5	**Indeterminate receive**	Client sends messages with a Content Length of zero and spreads the message out over a long period of time, unnecessarily using up server resources.		
6	**Garbage messages**	Client repeatedly sends invalid SIP messages.		
7	**Server congestion**	Client sends messages at a rate faster than what the server can handle. Further, client creates many open transactions.		
8	**Network congestion**	Client changes TCP receive window and uses Nagle algorithm (delayed ACK) with an aim to tying up server resources and effectively slowing it down		

9.2. Detailed Description of Limitations

Failure Point	
Phone type (if phone-specific)	
Call scenarios(s) associated with failure point	

List of UM features affected by failure point	
Additional Comments	

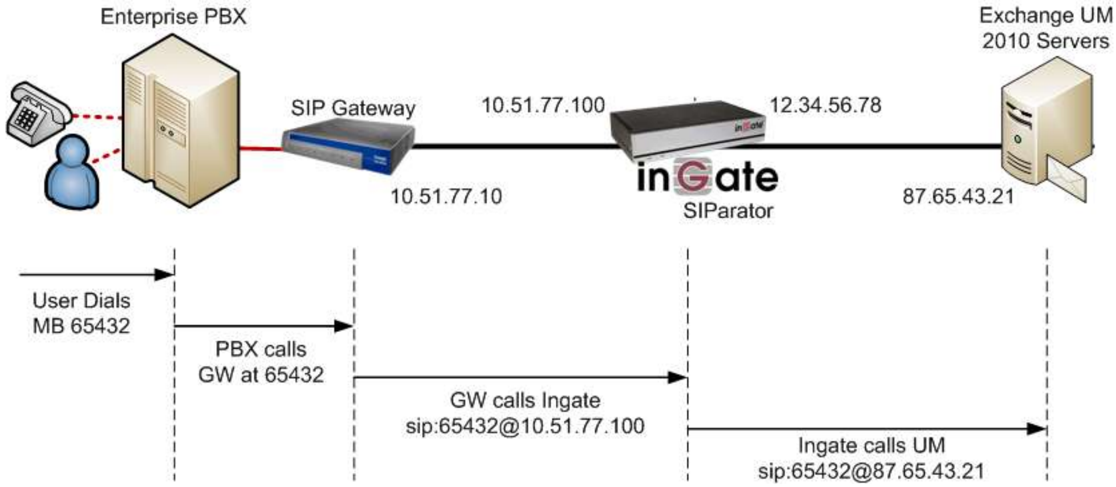
Failure Point	
Phone type (if phone-specific)	
Call scenarios(s) associated with failure point	
List of UM features affected by failure point	
Additional Comments	

10. Troubleshooting

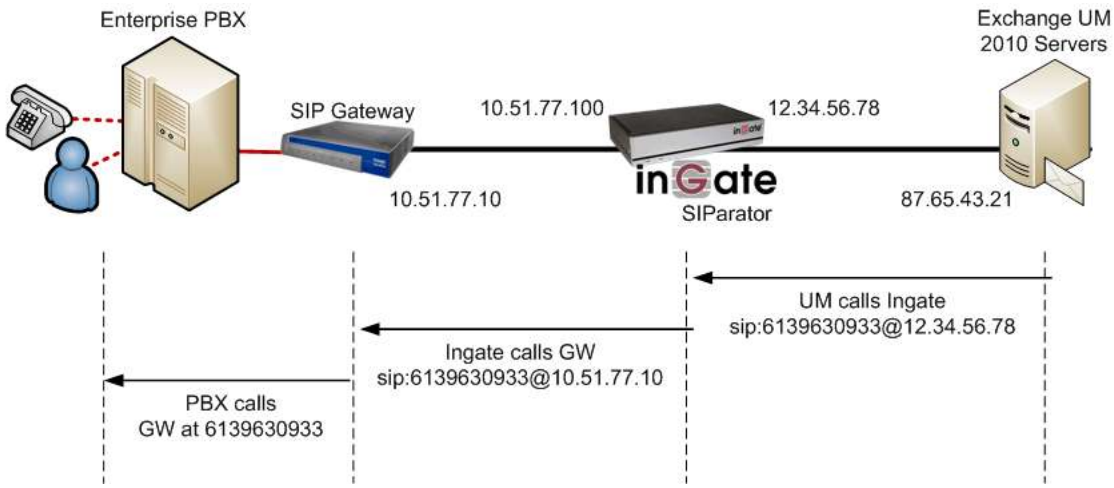
This section should provide some tips for troubleshooting problems, including troubleshooting commands and tools.

10.1. SIP Gateway to Ingate to UM Call Flow

For an Incoming call the call starts at the PBX, they will deliver a Mailbox number, this Mailbox number is contained in the Request URI header of a SIP INVITE out of the SIP Gateway. Typically the SIP Gateway will send an INVITE to the SIP URI address of "MailBox@IP_Address_of_Ingate". The Ingate then processes this through the Dial Plan and forwards the INVITE to the SIP URI address "Mailbox@IP_Address_UM".



For an outgoing call the call starts at the Exchange UM, they will deliver a DID contained in the Request URI header of a SIP INVITE. Typically the Exchange UM will send an INVITE to the SIP URI address of "DID@WAN_IP_Address_of_Ingate". The Ingate then processes this through the Dial Plan and forwards the INVITE to the SIP URI address "DID@IP_Address_GW".



Note: This works the same with an FQDN in the SPI Domains of the Request URI.

10.2. Startup Tool Troubleshooting

10.2.1. 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.

10.2.2. 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.
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

Possible Problems	Possible Resolution
	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.

10.2.3. Change or Update Configuration

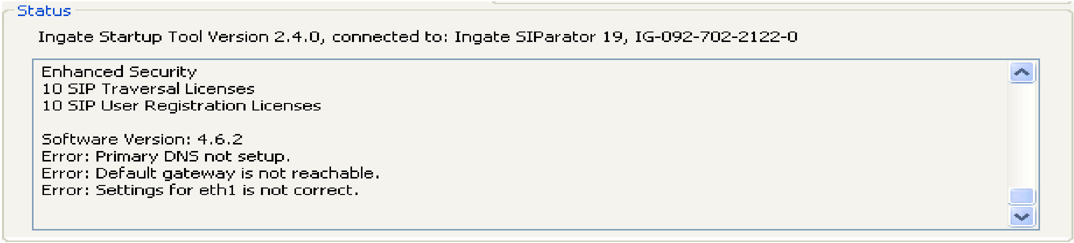
If the Ingate already has an IP Address and Password assigned to it, then you should be able use a Web Browser to reach the Ingate Web GUI. If you are able to use your Web Browser to access the Ingate Unit, then the Startup should be able to contact the Ingate unit as well. The Startup Tool will respond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

10.2.4. 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.



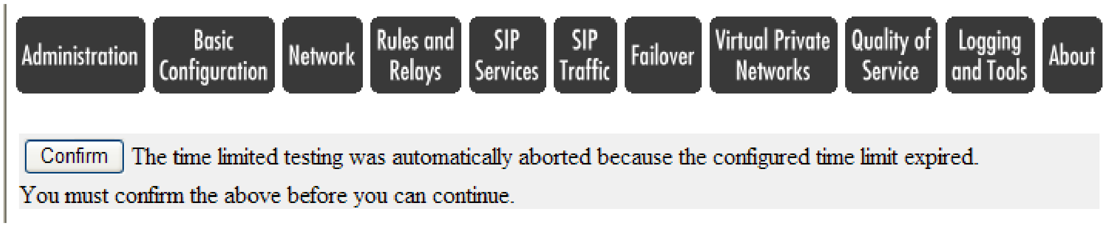
Possible Problems and Resolutions

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	IP Address of Netmask is in an Invalid

Possible Problems	Possible Resolution
correct.	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

10.2.5. 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.



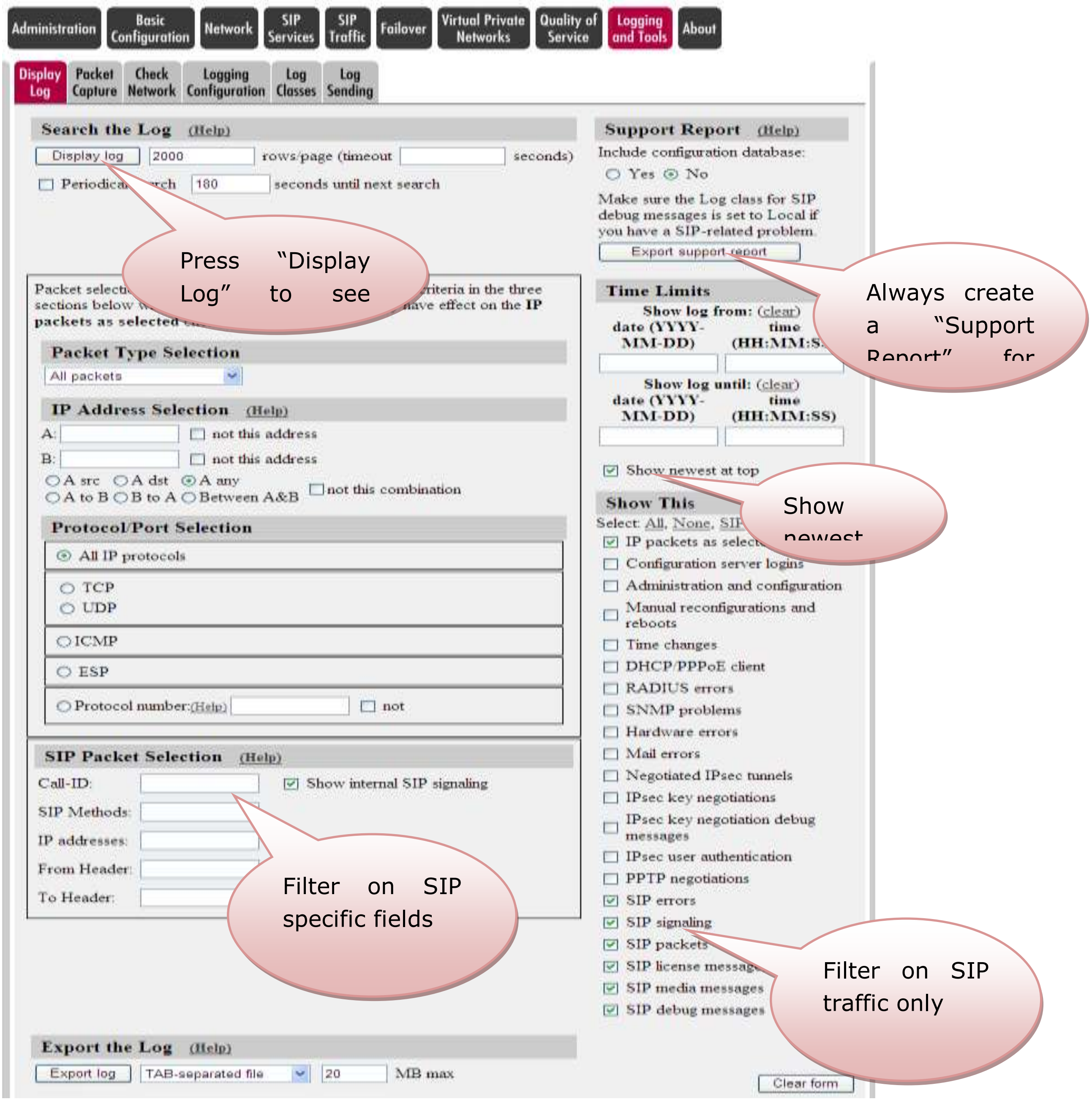
Possible Problems and Resolutions

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.

10.3. Ingate Troubleshooting Tools

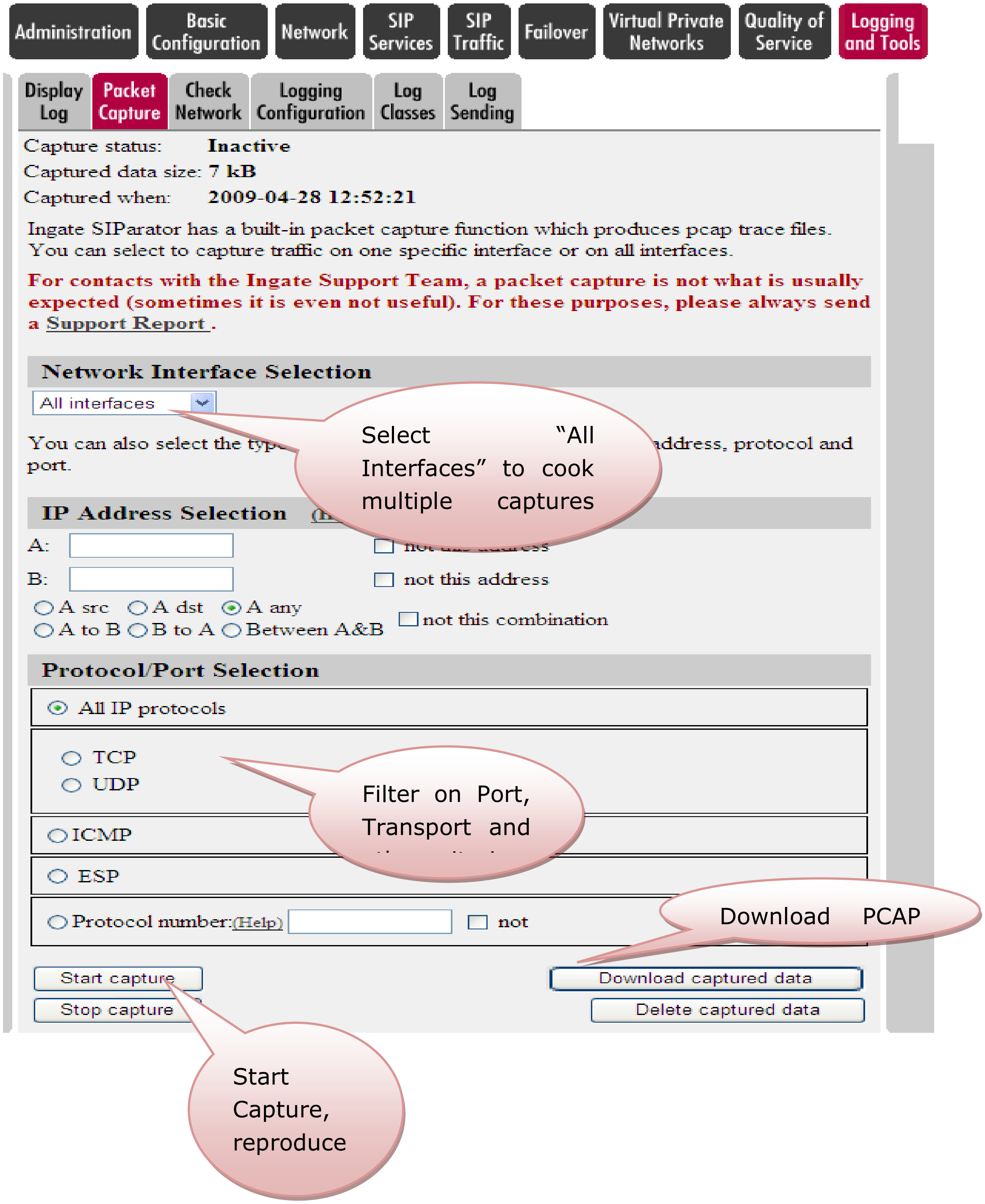
10.3.1. Display Logs

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



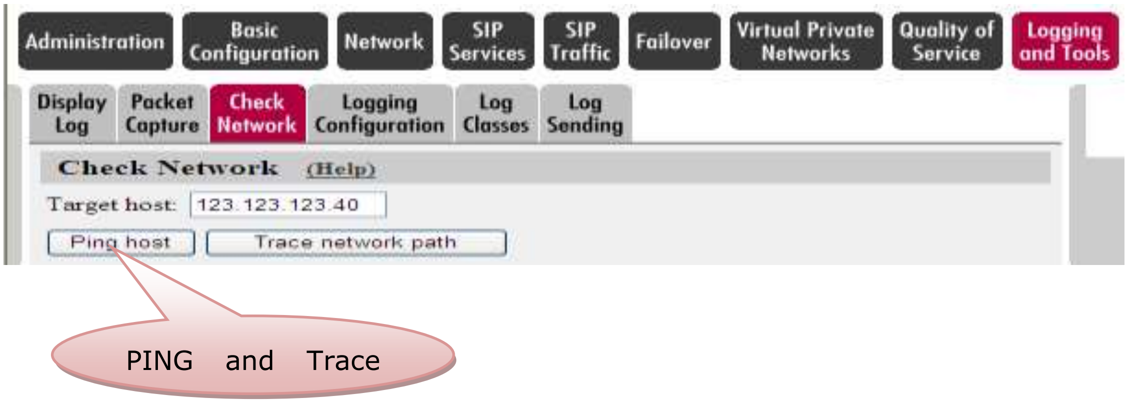
10.3.2. Packet Capture

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 you PC where it can be viewed in Wireshark or Ethereal.


Administration
Basic Configuration
Network
SIP Services
SIP Traffic
Failover
Virtual Private Networks
Quality of Service
Logging and Tools
Display Log
Packet Capture
Check Network
Logging Configuration
Log Classes
Log 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 Support Report .
Network Interface Selection
All interfaces
Select "All Interfaces" to cook multiple captures
IP Address Selection
A:
B:
not this address
A src
A dst
A any
A to B
B to A
Between A&B
not this combination
Protocol/Port Selection
All IP protocols
TCP
UDP
Filter on Port, Transport and
ICMP
ESP
Protocol number:(Help)
not
Download PCAP
Start capture
Stop capture
Download captured data
Delete captured data
Start Capture, reproduce

10.3.3. Check Network

Standard PING and Trace Route feature for simple network checks.



Appendix

1. Dial Pilot Number and Mailbox Login

- Dial the pilot number of the UM server from an extension that is NOT enabled for UM.
- Confirm hearing the greeting prompt: “Welcome, you are connected to Microsoft Exchange. To access your mailbox, enter your extension...”
- Enter the extension, followed by the mailbox PIN of an UM-enabled user.
- Confirm successful logon to the user’s mailbox.

2. Navigate Mailbox using Voice User Interface (VUI)

- Logon to a user’s UM mailbox.
- If the user preference has been set to DTMF tones, activate the Voice User Interface (VUI) under personal options.
- Navigate through the mailbox and try out various voice commands to confirm that the VUI is working properly.
- This test confirms that the RTP is flowing in both directions and speech recognition is working properly.

3. Navigate Mailbox using Telephony User Interface (TUI)

- Logon to a user’s UM mailbox.
- If the user preference has been set to voice, press “#0” to activate the Telephony User Interface (TUI).
- Navigate through the mailbox and try out the various key commands to confirm that the TUI is working properly.
- This test confirms that both the voice RTP and DTMF RTP (RFC 2833) are flowing in both directions.

4. Dial User Extension and Leave Voicemail

- Note: If you are having difficulty reaching the user’s UM voicemail, verify that the coverage path for the UM-enabled user’s phone is set to the pilot number of the UM server.

a. From an Internal Extension

- From an internal extension, dial the extension for a UM-enabled user and leave a voicemail message.
- Confirm the voicemail message arrives in the called user's inbox.
- Confirm this message displays a valid Active Directory name as the sender of this voicemail.

b. From an External Phone

- From an external phone, dial the extension for a UM-enabled user and leave a voicemail message.
- Confirm the voicemail message arrives in the called user's inbox.
- Confirm this message displays the phone number as the sender of this voicemail.

5. Dial Auto Attendant(AA)

- Create an Auto Attendant using the Exchange Management Console:
  - Under the Exchange Management Console, expand "Organizational Configuration" and then click on "Unified Messaging".
  - Go to the Auto Attendant tab under the results pane.
  - Click on the "New Auto Attendant…" under the action pane to invoke the AA wizard.
  - Associate the AA with the appropriate dial plan and assign an extension for the AA.
  - Create SBC dialing rules to always forward calls for the AA extension to the UM server.
  - Confirm the AA extension is displayed in the diversion information of the SIP Invite.
- Dial the extension of Auto Attendant.
- Confirm the AA answers the call.

6. Call Transfer by Directory Search

- Method one: Pilot Number Access
    - Dial the pilot number for the UM server from a phone that is NOT enabled for UM.
    - To search for a user by name:
    - Press # to be transferred to name Directory Search.

        - Call Transfer by Directory Search by entering the name of a user in the same Dial Plan using the telephone keypad, last name first.
    - To search for a user by email alias:
        - Press “#” to be transferred to name Directory Search
        - Press “# #” to be transferred to email alias Directory Search
        - Call Transfer by Directory Search by entering the email alias of a user in the same Dial Plan using the telephone keypad, last name first.
- Method two: Auto Attendant
    - Follow the instructions in appendix section 5 to setup the AA.
    - Call Transfer by Directory Search by speaking the name of a user in the same Dial Plan. If the AA is not speech enabled, type in the name using the telephone keypad.
- Note: Even though some keys are associated with three or four numbers, for each letter, each key only needs to be pressed once regardless of the letter you want. Ignore spaces and symbols when spelling the name or email alias.

a. Called Party Answers

- Call Transfer by Directory Search to a user in the same dial plan and have the called party answer.
- Confirm the call is transferred successfully.

b. Called Party is Busy

- Call Transfer by Directory Search to a user in the same dial plan when the called party is busy.
- Confirm the calling user is routed to the correct voicemail.

c. Called Party does not Answer

- Call Transfer by Directory Search to a user in the same dial plan and have the called party not answer the call.
- Confirm the calling user is routed to the correct voicemail.

d. The Extension is Invalid

- Assign an invalid extension to a user in the same dial plan. An invalid extension has the same number of digits as the user’s dial plan and has not been mapped on the SBC to any user or device.

    - UM Enable a user by invoking the “Enable-UMMailbox” wizard.
    - Assign an unused extension to the user.
    - Do not map the extension on the SBC to any user or device.
    - Call Transfer by Directory Search to this user.
    - Confirm the call fails and the caller is prompted with appropriate messages.

7. Play-On-Phone

- To access play-on-phone:
    - Logon to Outlook Web Access (OWA) by going to URL https://<server name>/owa.
    - After receiving a voicemail in the OWA inbox, open this voicemail message.
    - At the top of this message, look for the Play-On-Phone field (Play on Phone...).
    - Click this field to access the Play-On-Phone feature.

a. To an Internal Extension

- Dial the extension for a UM-enabled user and leave a voicemail message.
- Logon to this called user’s mailbox in OWA.
- Once it is received in the user’s inbox, use OWA’s Play-On-Phone to dial an internal extension.
- Confirm the voicemail is delivered to the correct internal extension.

b. To an External Phone number

- Dial the extension for a UM-enabled user and leave a voicemail message.
- Logon to the UM-enabled user’s mailbox in OWA.
- Confirm the voicemail is received in the user’s mailbox.
- Use OWA’s Play-On-Phone to dial an external phone number.
- Confirm the voicemail is delivered to the correct external phone number.
- Troubleshooting:
    - Make sure the appropriate UMMailboxPolicy dialing rule is configured to make this call. As an example, open an Exchange Management Shell and type in the following commands:
    - $dp = get-umdialplan -id <dial plan ID>

- $dp.ConfiguredInCountryOrRegionGroups.Clear()
- $dp.ConfiguredInCountryOrRegionGroups.Add("anywhere,*,*,")
- $dp.AllowedInCountryOrRegionGroups.Clear()
- $dp.AllowedInCountryOrRegionGroups.Add(“anywhere")
- $dp|set-umdialplan
- $mp = get-ummailboxpolicy -id <mailbox policy ID>
- $mp.AllowedInCountryGroups.Clear()
- $mp.AllowedInCountryGroups.Add("anywhere")
- $mp|set-ummailboxpolicy
- The user must be enabled for external dialing on the SBC.
- Depending on how the SBC is configured, you may need to prepend the trunk access code (e.g. 9) to the external phone number.

8. Call Route across Forest

- To route call across forest:
  - Dial pilot number of the UM server.
  - Confirmed that Moved (302) sip message is returned with the right UM server FQDN.
  - Make sure SBC made call to the right forest.
  - If the SBC has an option to redirect the 302 back to gateway, configure SBC such like that 302 message is sent back to gateway.
  - Make sure that Gateway made call to right forest.