How To Configure the Ingate® SIParator®/Firewall E-SBC with Microsoft® Lync® 2013, 2010 and OCS 2007

February 2015

Table of Content

Revision History:

Revision	Date	Author	Comments
	2012-12-14	Gino Larenas	First draft
15B	2015-02-28	KES, Zlatan Klapic	Updates

1 Introduction

This document describes how to configure Ingate's SIParator® devices to work as Session Border Controllers for connecting Microsoft® Lync® to an ITSP.

1.1 Before you Begin

To complete this checklist, you will need the following software and hardware:

From Ingate:

- Any Ingate SIParator / Firewall appliance or software version, using current software. Before ordering, determine the capacity (the maximum number of concurrent calls) required by your organization, and then specify the required capacity when ordering. Capacity determines Model selection. For assistance in determining required capacity, please visit Microsoft's site
- Current Ingate SIParator software (5.0.5 or later). Lab qualified Lync compliance was introduced with version 4.10.2, but upgrading to the latest version is strongly recommended.
- Ingate SIParator SIP Trunking Module[1]

From Microsoft:

- Lync Standard or Enterprise Edition.

From ITSP:

- SIP Trunk to IP telephony provider (optionally with TLS/SRTP support, but not required)

1.2 Compatibility and Limitations

The Ingate SIParator / Firewall E-SBC has been successfully installed with the ITSPs found at: http://www.ingate.com/Confirmed_ITSP.php (Using the Ingate E-SBC at the Enterprise edge, ITSPs do not have to be Microsoft Lync-qualified in themselves.)

The Ingate SIParator / Firewall E-SBC has been successfully installed with the PBXs found at: https://www.ingate.com/Confirmed_IP-PBX.php

The Ingate SIParator / Firewall E-SBC has been qualified by Microsoft accredited test lab against the complete Lync 2010 test suite including all options (TLS/SRTP, Failover, Transfer and Call Park tests). In addition, the Ingate products can transcode signaling between UDP/TCP/TLS and media between RTP/SRTP.

The Ingate SIParator / Firewall E-SBC is also used by service providers (ITSPs) and has been qualified by Microsoft accredited test lab against the complete Lync 2010 test suite for an ITSP including all options (i.a. TLS/SRTP).

---

[1] The Ingate SIParator Enhanced Security module is also required, but is automatically included with recent versions of the SIParator/Firewall software. You can check that the Enhanced Security is included under the **About** tab in the administration GUI.

The Lync 2013 test suite made TLS/SRTP support mandatory and added optional IPv6 tests. Ingate has verified conformance to all these tests, but optional IPv6 (including IPv6 to IPv4 transcoding for both signaling and media) is planned to be available in a future Ingate software update).

The Ingate SIParator / Firewall E-SBC also works with the Lync predecessor, OCS 2007 and is expected to also be compatible with upcoming Lync 2015 or Skype for Business as it may be named.

Full compatibility with all combinations of ITSPs (current and future versions), Lync versions and PBXs cannot be guaranteed, but are most likely using the Ingate product. Installers are expected to be familiar with the Ingate product, and installation support is recommended to be purchased, especially when working with a new combination.

This guide focuses of connecting Lync to an ITSP. For additional integration with a PBX, PBX installation steps will also be required and other guides or support may have to be consulted. This also applies to more complex network scenarios.

2 How an Ingate SIParator SBC fits into your Lync Deployment

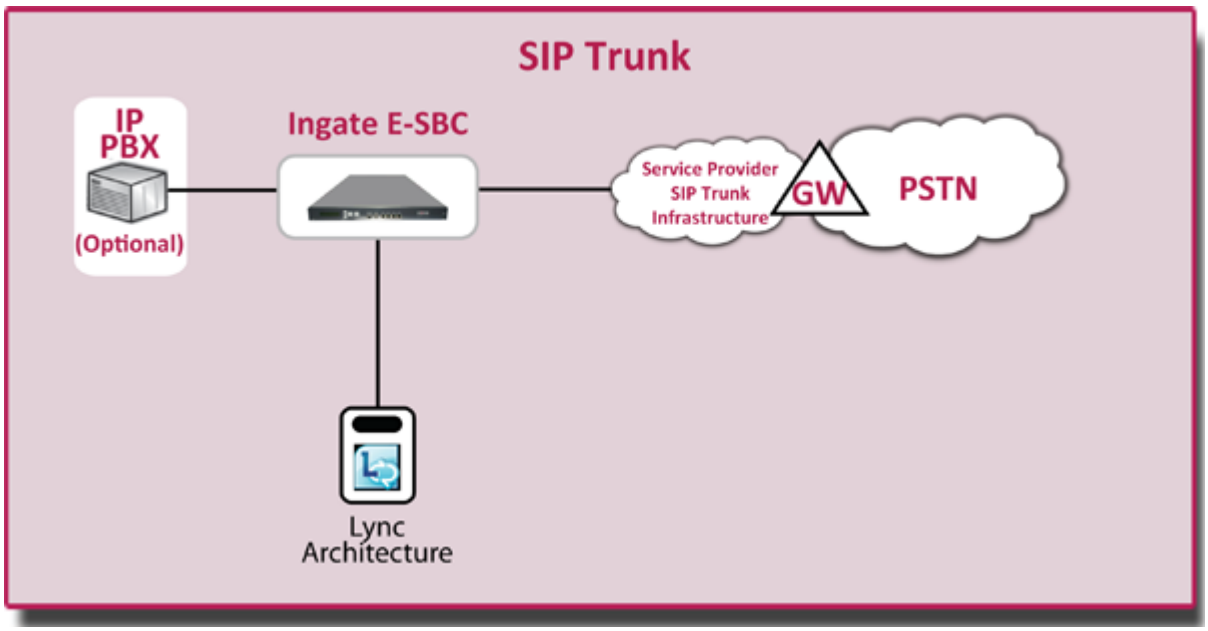


Figure 1: How the Ingate SIParator SBC fits into your Lync Deployment

The Ingate E-SBC is functionally connected to the mediation server of the Lync architecture, as shown by the picture above. The Ingate E-SBC contains its own firewall and does not require the internal and external firewalls of a DMZ, often shown in Lync setups. The Ingate product provides all protection of the enterprise LAN, the ITSP and itself, with or without such DMZ installation.

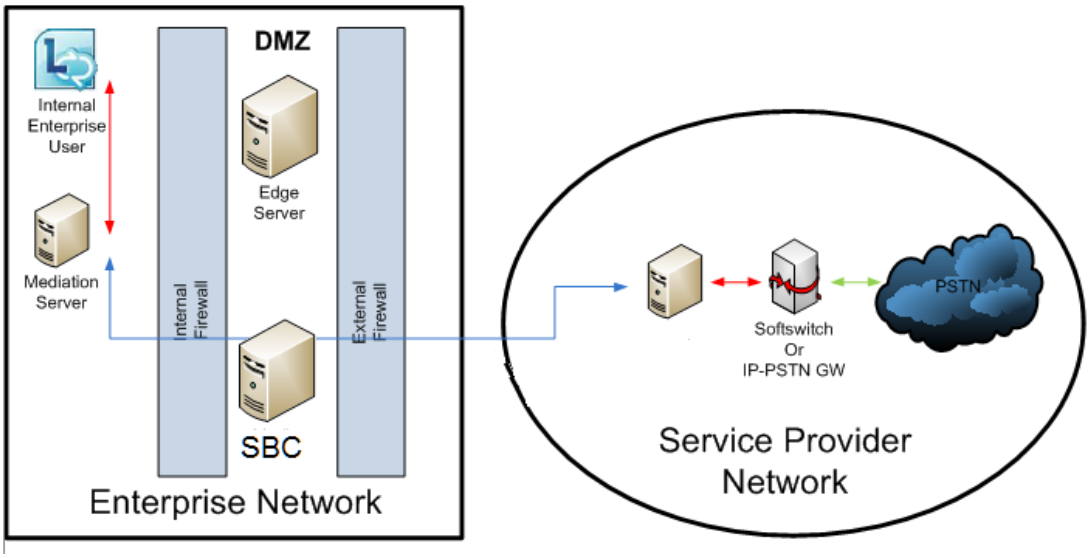


Figure 2: The Ingate SIParator may be deployed in the DMZ, but it is not required (like it is with some other products not having full security features), since the SIParator includes its own firewall.

If the E-SBC is installed in a DMZ, then make sure the IP addresses and ports used by SIP are open (and without NAT) towards the Lync mediation server and towards the service provider. If the Lync mediation server is behind another router on the LAN-side, a static route must be added to the Ingate E-SBC routing table.

In addition to firewall/NAT traversal and security, the Ingate SIParator provides SIP interoperability (SIP normalization) as well as signaling (UDP/TCP/TLS) and media (RTP/SRTP) transcoding between different SIP components in the UC (Unified Communications) infrastructure.

3 Configuration Checklist

You will need to complete the following steps in order to configure an Ingate SIParator Session Border Controller (SBC), Lync and your SIP Trunking Service Provider to work together. You need to configure DNS and UM first, and then configure the SBC to route traffic to and from Lync.

- Configure Lync to work with a Session Border Controller
- Set up and connect the SBC
- Do initial configuration on the SBC
- Verify SBC configuration

This document describes an Ingate SIParator configuration that will work with Microsoft Lync. It assumes that you have one SIParator unit, and one installation of Lync Standard or Enterprise Edition. It also describes how to use optional signaling TLS and media SRTP encryption for enhanced security. If you have more complex requirements (e.g. multiple SIParators for high availability), please consult the Ingate documentation for details.

4 Step 1: Configure Lync to work with an E-SBC

This guide assumes you have knowledge on how to configure Lync for SIP Trunking. For SIP Trunking, the E-SBC is connected to the mediation server in the Lync Architecture.

E.g. see: Deploying Enterprise Voice in Lync Server 2013

Full information is available at the Microsoft Website.

For OCS (predecessor of Lync) you may also see Ingate's Configuration Guide for Microsoft OCS 2007

5 Step 2: Set Up and Connect the SIParator

5.1 Hardware and Network Setup

After connecting power, connect an Ethernet cable to the port marked **Eth0** of the device. This cable must be connected to your private IP network: the **Eth0** port will be used to configure the unit with the Ingate Startup Tool (See examples below. For other Ingate models, their documentation may have to be consulted.).

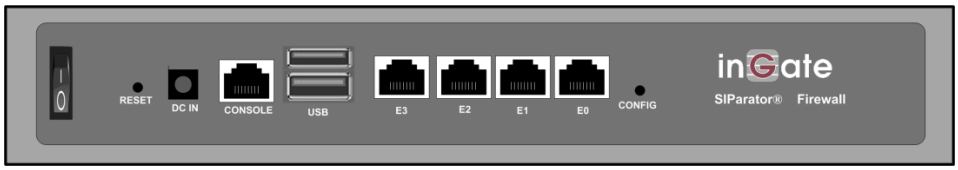


Figure 3. Back panel of Ingate SIParator 21 / Firewall 1210

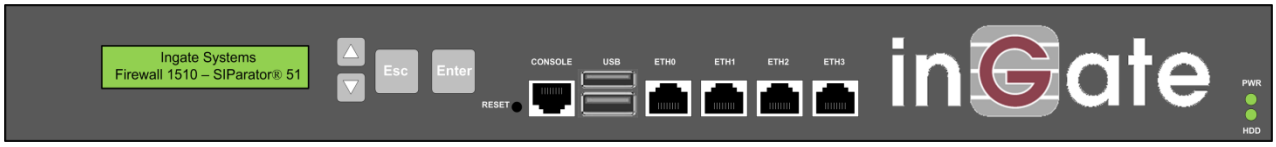


Figure 4. Front panel of Ingate SIParator 51, 56, 66 /Firewall 1510, 1560, 1660

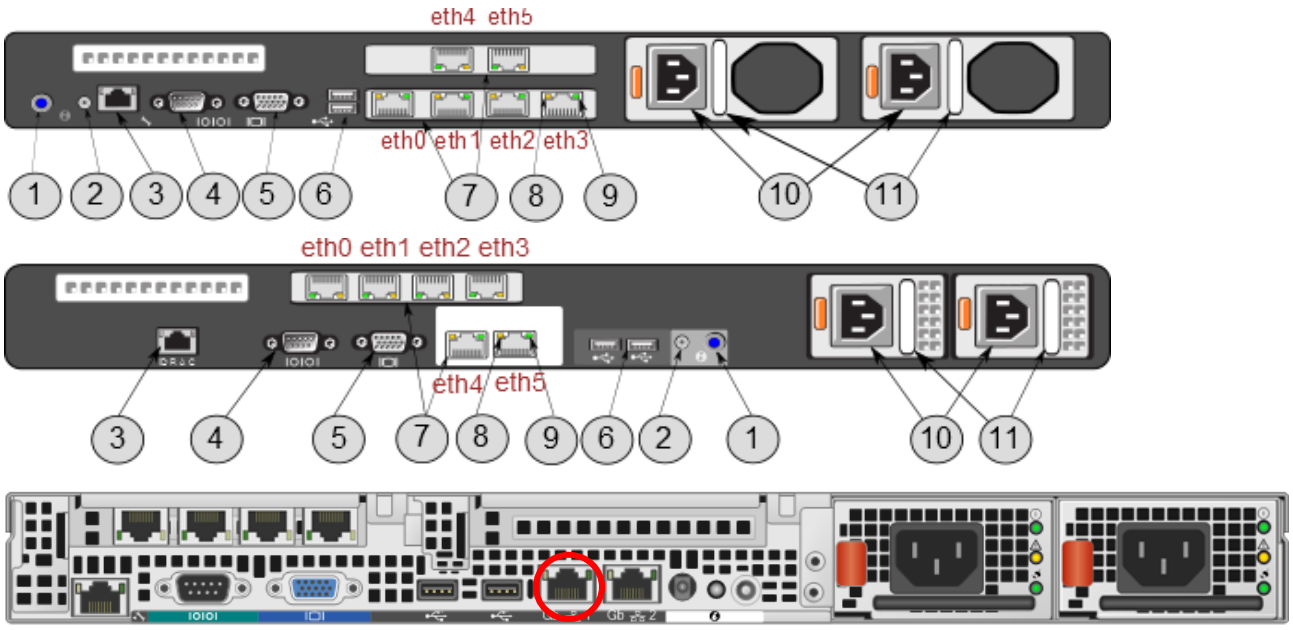


Figure 5. Back panels of Ingate SIParator 95, 96, 97, 98 / Firewall 1950, 1960, 1970, 1980

The Ingate Startup Tool is an "Out-of-the-Box" commissioning tool and is not a "Config-Everything" tool. It assumes a typical networking topology and basic setup requirements.

When you connect the SIParator to the external (public IP) network, plug an Ethernet cable into the port marked **Eth1**.

This configuration note and the Ingate Startup Tool assumes that **all of the following are connected to the same subnet on the private IP network:**

- SIParator (via port **Eth0**)
- Lync front end servers (mediation servers) Standard Edition or Enterprise
- Computer running the Ingate Startup Tool

If, for some reason, this is not the case, the Startup Tool will restrict to Gateways and IP-PBX IP Addresses to the local Subnet of the Ingate. This can be easily changed later on the Ingate Administration GUI. Then you should consult the Ingate Reference Manual (Chapter 6 – Interface: Static Routing) for additional network setup (adding a static route).

5.2 Ingate Startup Tool (SUT)

5.2.1 First Time Setup of the SIParator

Before you can administer the device, you must configure its IP address and administrative password with the Ingate Startup Tool. The tool must run on a PC that is located on the same LAN subnet as the device itself (rather than, for example, a different subnet, across routers, or through a VPN tunnel).

The tool can be downloaded free of charge at http://www.ingate.com/Startup_Tool.php. Make sure to download the "SUT TG" version (the earlier version, not supporting Trunk

Groups is obsolete). (The screenshots and detailed description relates to version 1.1.1 and details may vary.)

Next, launch the tool.

Select the model type of the Ingate unit as **Ingate Firewall/SIParator** (Figure 6) and click **Next**.

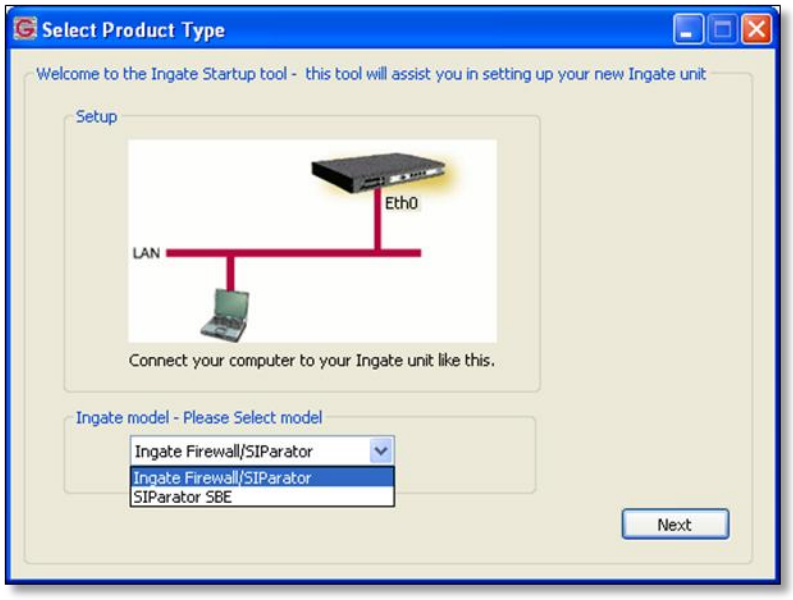


Figure 6. Device selection screen

You will see a configuration page (Figure 7).

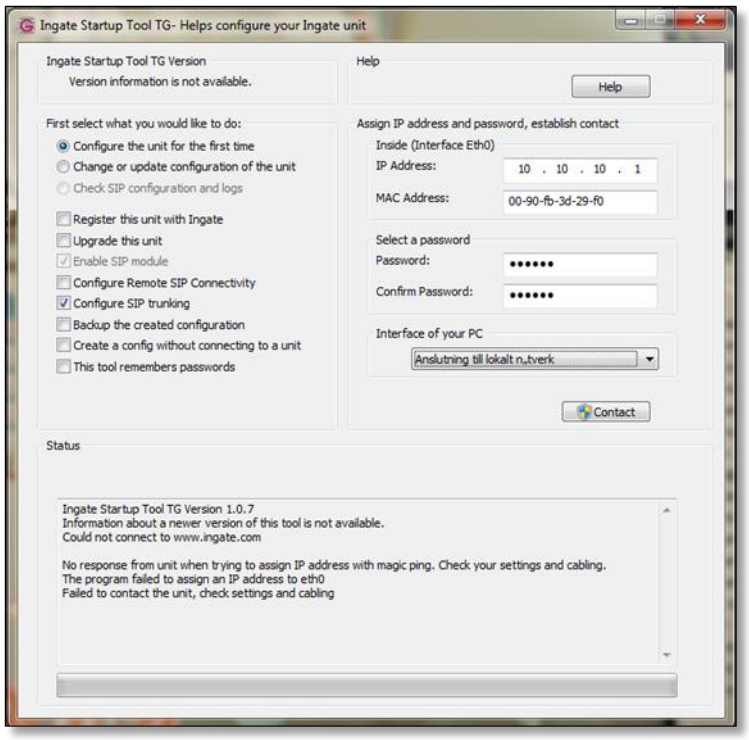


Figure 7. First time configuration

In the group box labeled **First select what you would like to do**, select the radio button labeled **Configure the unit for the first time**.

In the group box labeled **Inside (Interface Eth0)**, go to the **IP Address** field and enter a static IP address by which the **Eth0** interface will be addressed on your private network. Then, go to the **MAC Address** field and enter the address that will be found on a sticker attached to the unit. Figure 8 shows an example.

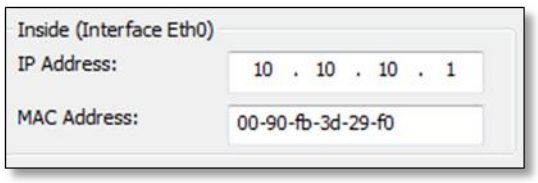


Figure 8: IP and MAC address assignment

In the group box labeled **Select a Password**, enter (and confirm) the password which will be used to authenticate administrators of the device, (Figure 9).

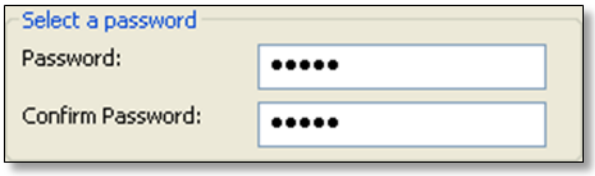


Figure 9: Password assignment

In the drop-down list labeled **Interface of your PC**, select the network interface (e.g. **Local Area Connection**) that you wish to use to communicate with the SIParator (Figure 10).

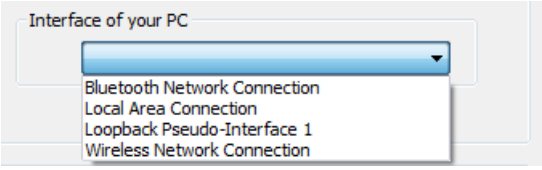


Figure 10. Selecting the network interface used by the Startup Tool

When these values have been entered, the **Contact** button at the bottom right of the form (Figure 7) will become active.

Press the **Contact** button.

The Startup Tool will find the Ingate unit on the network and communicate with it and assign its IP address and password.

5.2.2 Network Topology

The Ingate SIParator device supports many different configuration modes and functions.

Go to the **Network Topology** tab.

In the **Product Type** drop down list, select **Standalone SIParator** (Figure 11) if your network topology is as indicated by the picture to the right of the list (Figure 13). Otherwise, select the type that fits your network topology. (The LAN SIParator should typically be avoided, as it requires non trivial configuration and functions of the enterprise firewall.)

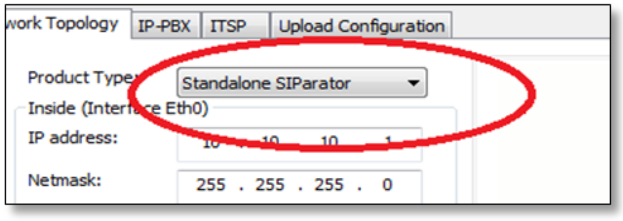


Figure 11. Configuring Product Type

After configuring the type, the controls on the administrative interface will change, according to the type selected (Figure 13).

The internal network interface details, listed in the in the group box labeled **Inside (Interface Eth0)**, should be consistent with your earlier assignment. These represent the device's interface to your private IP network.

Details of the device's interface to the public IP network can be configured with the controls in the group box labeled **Outside (Interface Eth1)**.

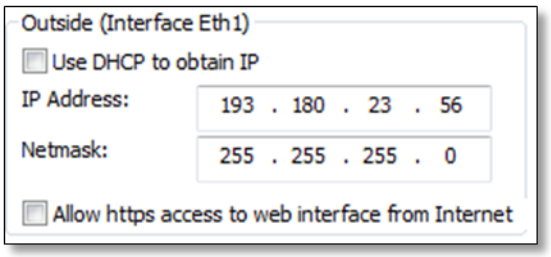


Figure 12. Configuring the external network interface

Once you have entered the internal and external interface details (IP Address/Netmask), in the **Gateway section** below enter the address of the router that acts as a firewall gateway for your network.

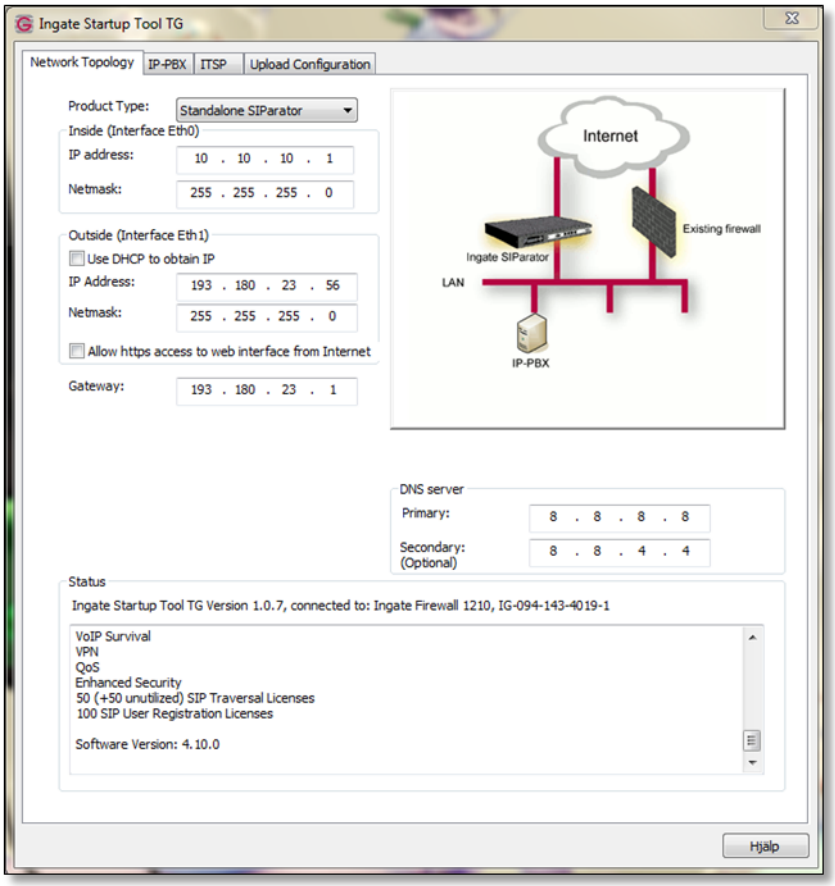


Figure 13. Configuring Network Topology

Finally, enter the **DNS server** IP addresses. These can be internal or external.

6 Step 3: The Initial Configuration of the SIParator

Microsoft Lync supports SIP signaling transport over TCP and TLS, but not UDP. The Startup Tool will setup TCP, and later – if TLS signaling is preferred – certificates will imported into the SIParator and TLS enabled.

6.1 IP-PBX Configuration

In the Ingate Startup Tool, navigate to the **IP-PBX** tab (Figure 14).

This configuration is related to the SBC's connection, via its internal interface, to the VoIP gateway or IP PBX.

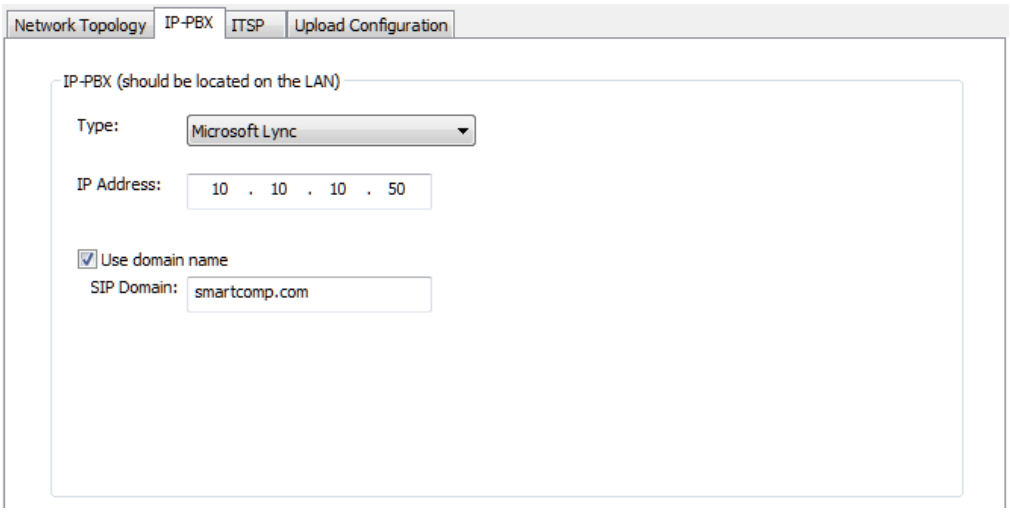


Figure 14. Choosing Lync as IP-PBX

In the **Type** drop-down list, select **Microsoft Lync** as your IP PBX

In the **IP Address** field, enter the address of the IP PBX or gateway on your network

In the **SIP Domain** enter Lync's FQDN or Pool name (This step is optional if only IP address is used).

If the Lync mediation server is behind another router on the LAN-side, you may have to set a local dummy IP address, not to be blocked by the Startup Tool and later, in the Ingate administration web GUI, change it and also add a static route to the Ingate E-SBC routing table. See 7.2.1 The Lync Mediation Server on Another Subnet

6.2 ITSP Configuration

In the Ingate Startup Tool, navigate to the **ITSP** tab (Figure 15).

This is to connect the SIParator to the ITSP (Internet Telephony Service Provider) via its external interface.

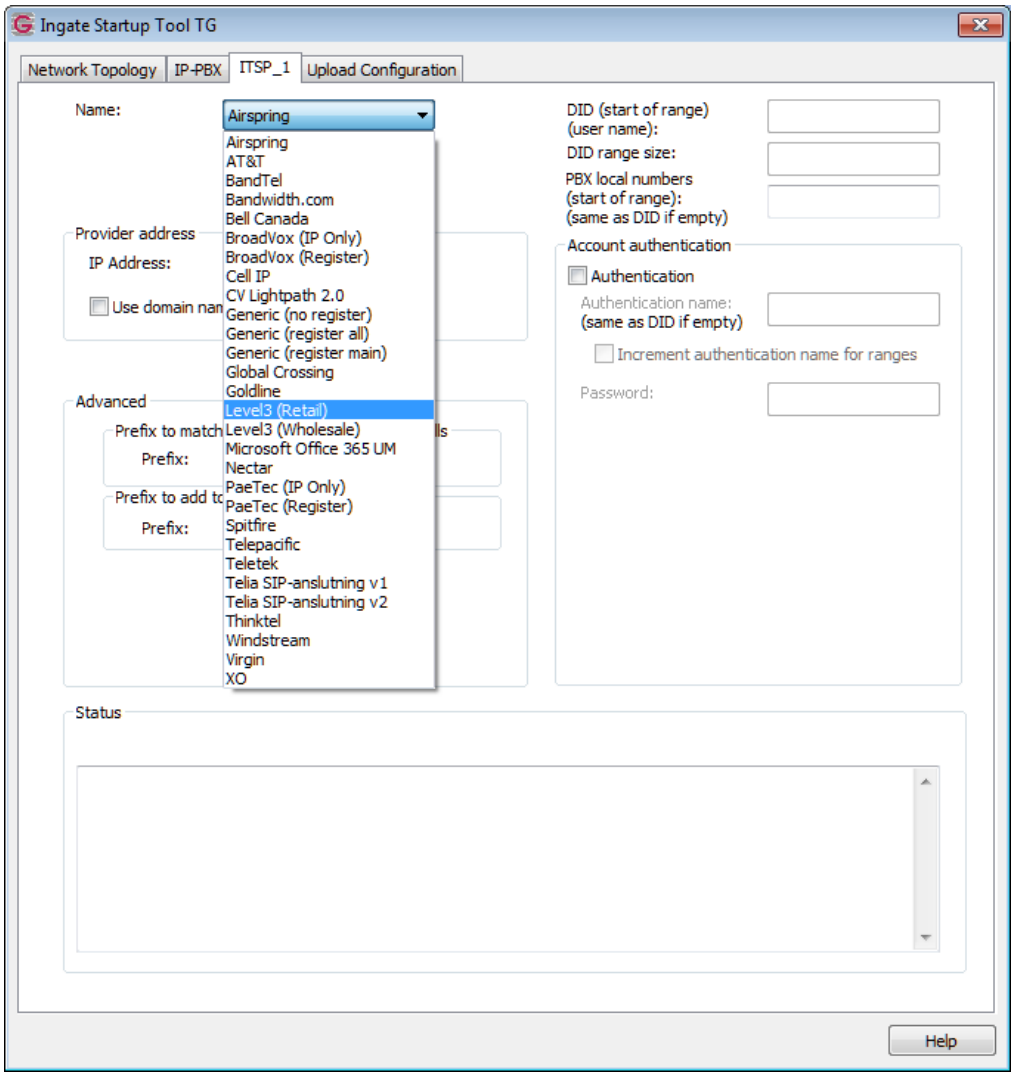
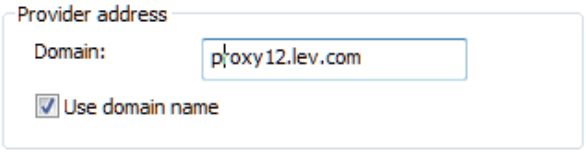


Figure 16. Configuring the external SIP interface details

In the **Name** drop-down list, select your ITSP. If your ITSP is not available, you may try one of **Generic ITSPs**. For a non-available ITSP, you need to have the specification of the SIP Trunk service from the ITSP and first of all select whether the SIParator shall register to the service and if it should, whether only the main number or all DIDs shall register. Additional manual configuration may also be required to achieve full interoperability.

Figure 17. Selecting a Generic ITSP not requiring registration to the SIP service when the ITSP is not available in the list.

Thereafter, choose IP address or FQDN for the ITSP in the **Provider address** group



or

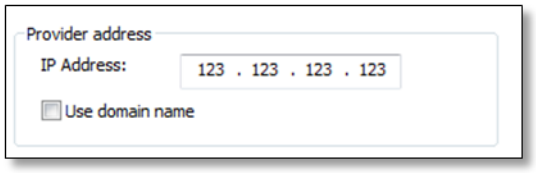


Figure 18. Configuring the address of the ITSP

6.3 Uploading the Configuration

When you have completed the previous configuration steps, the Start Up Tool will load the configuration data into the Ingate SIParator. The tool can also be used to create a backup configuration file for later use.

In the tool, navigate to the **Upload Configuration** tab (Figure 19).

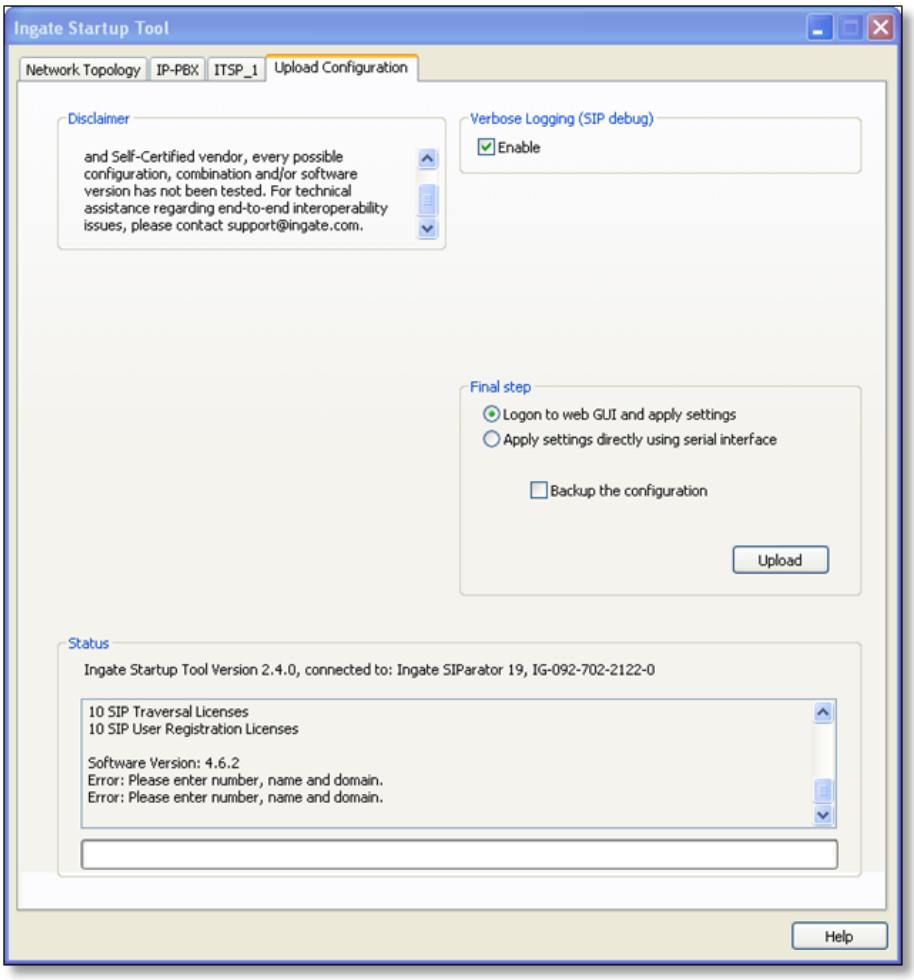


Figure 19. Uploading configuration data to the SIParator

In the **Final step** controls, ensure that the radio button labeled **Login to the web GUI and apply settings** is selected.

If you would like the tool to create a backup file, check the box labeled **Backup the configuration**.

Click the **Upload** button.

The configuration data will be copied from the startup tool to the SIParator.

When the data has been uploaded, a dialog box will appear (Figure 20).

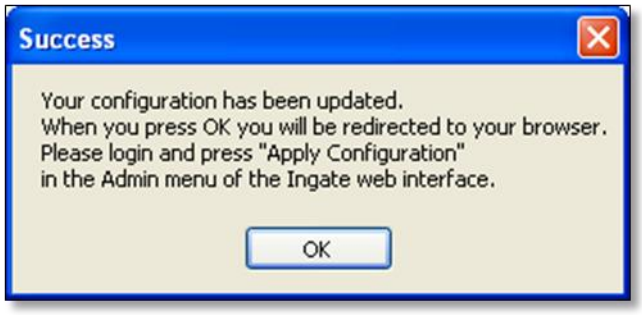


Figure 20. Confirmation of configuration data upload

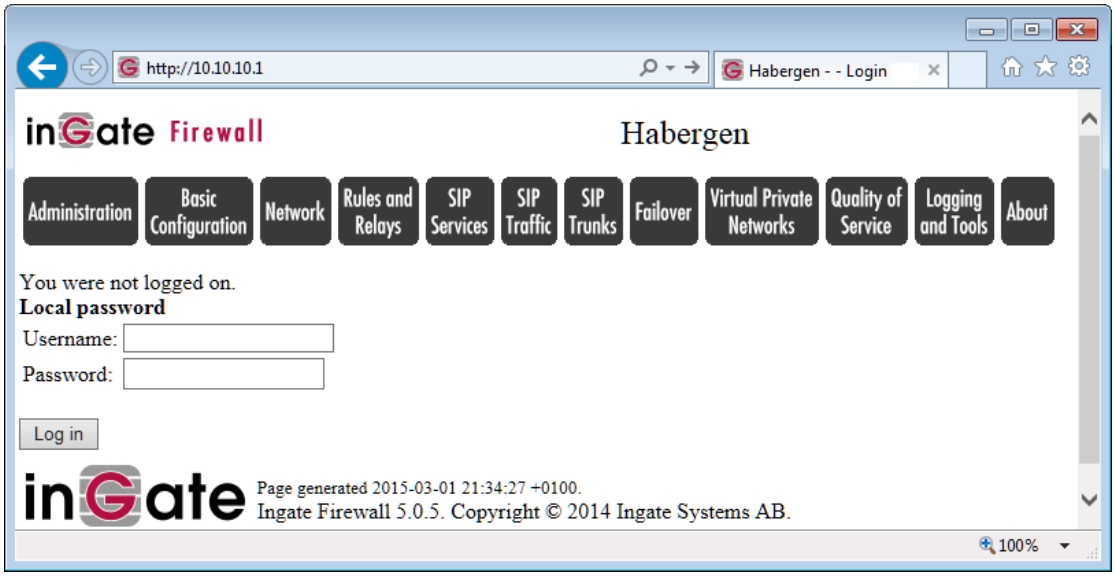
Click on **OK**. The default web browser will launch and navigate you to the SIParator's administration web interface.

7 Administration Web GUI (Graphical User Interface)

7.1 Applying the Configuration

Although the configuration data has been uploaded to the SBC, it must be explicitly applied before it is activated in the SIParator.

You log into the web interface with the administrative password that you selected earlier (page 9).



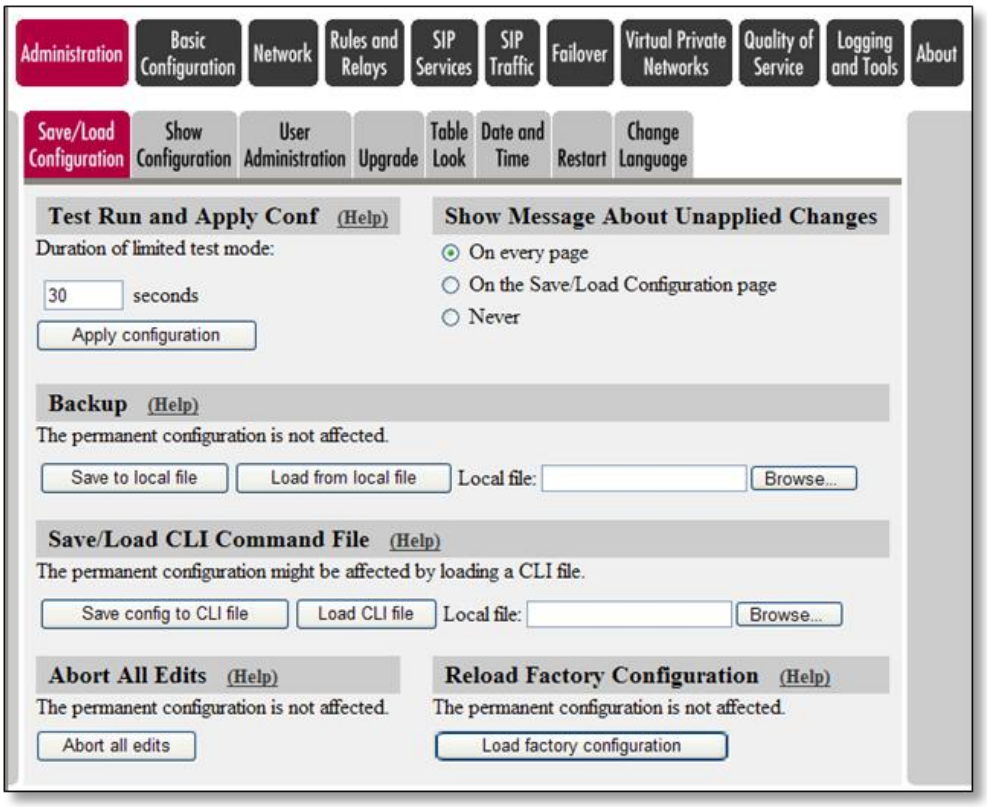


Figure 21. Applying the uploaded configuration

Under **Administration** > **Save/Load Configuration**, click the **Apply configuration** button.

A window will appear (Figure 22) requesting further input.

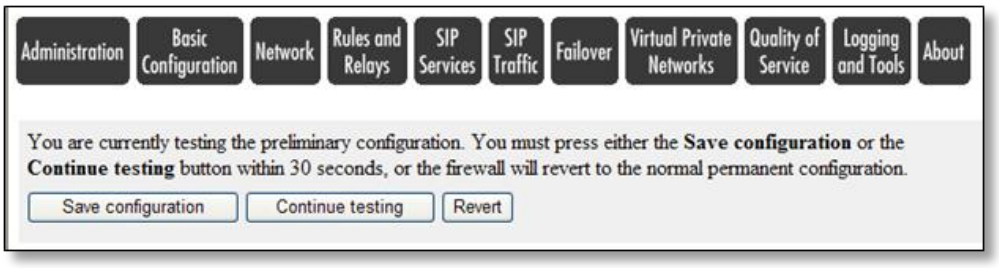


Figure 22. Saving the configuration

Click the button labeled **Save configuration**.

This completes the process of transferring and applying the configuration data to the SIParator device.

If further configuration is required, e.g. adding TLS with certificates, or any change to settings made by the Start Up Tool, it can be applied through this administration web interface.

7.2 Additional Manual Configuration Using the Web GUI

Manual configuration beyond the Start Up Tool configuration may be required e.g. if Generic ITSP selection is made.

Here we illustrated that the ITSP may have several servers at different IP addresses but you still (for enhanced security) may want to limit the IP address range used for the SIP communication.

Go to **Network** > **Network and Computers** and find the IP address of ITSP entered by the Start UP Tool in the row named "Generic (no register)". Here, you can change the lower and upper limit include the IP addresses of the SIP servers that the ITSP uses (as specified by the ITSP for the specific service offered).

Networks and Computers

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		
Generic (no regi	-	123.123.123.123	0.0.0.0		255.255.255.255	-	
Generic IP-PBX	-	[illegible]	10.10.10.50			-	
LAN	-	10.10.10.0	10.10.10.0	10.10.10.255	10.10.10.255	inside (eth0 untagged)	
WAN	-	0.0.0.0	0.0.0.0	255.255.255.255	255.255.255.255	outside (eth1 untagged)	

Add new rows 1 groups with 1 rows per group.

Thereafter, go to **SIP Trunks**> **Trunk 1**, select the Trunk from the drop down list and click Goto SIP Trunk page.

Under the **SIP Trunking Service,** change the field **Restrict calls from** to **Generic (no register).** The SIP Trunk group 1 will then only response to SIP requests from those limited IP addresses.

SIP Trunk 1 (Help)

Enable SIP Trunk
Disable SIP Trunk

SIP Trunking Service (Help)

Use parameters from other SIP trunk
Define SIP trunk parameters

Service name:	Generic (no register)	*(Descriptive name)*
Service Provider Domain:	123.123.123.123	*(FQDN or IP address)*
Restrict to calls from:	Generic (no register)	*('-' = No restriction)*
Outbound Proxy:		*(FQDN or IP address)*
Use alias IP address:	-	*(Forces this source address from our side)*
Outbound Gateway:	-	*('-' = Use Default Gateway)*
Signaling Transport:	-	*('-' = Automatic)*
Port number:		

Provider domain

Save settings and Apply configuration (as explained under 7.1 Applying the Configuration)

7.2.1 The Lync Mediation Server on Another Subnet

If the Lync mediation server of the Lync architecture is behind another router on the LAN-side, a static route must be added to the Ingate E-SBC routing table.

This is easily done now in the Ingate Administration GUI. You should consult the Ingate Reference Manual (Chapter 6 – Interface: Static Routing) for additional network setup (adding a static route).

8 Step 4: Optional TLS and SRTP Encryption and Using Certificates

8.1 Configuring TLS SIP Signaling Encryption

Transport Layer Security (TLS) can be used to secure the signaling between the SIParator and Lync, instead of plain TCP transport.

To configure TLS between the Ingate SIParator and Lync, the following conditions must be met:

A suitable **digital certificate** must be deployed on Ingate SIParator.

The **Enhanced SIP Security Module** required for TLS and SRTP encryption functionality is always included in recent versions of the Ingate SIParator software.

Configuring TLS and SRTP towards the ITSP is also a supported option, see section 8.6 Using TLS and SRTP over the ITSP SIP Trunk.

8.1.1 Configuring Certificates

You must obtain a digital certificate, signed by a supported Certification Authority (CA), which contains the FQDN of the SBC in the certificate's name (CN) field (in this case signed by the local Certification Authority Windows Domain Controller). This certificate must then be loaded into the SIParator. You must also upload the root certificate from your domain controller.

Follow these next steps:

1. The SBC's fully qualified domain name (FQDN) is what you configure in DNS to represent the SBC's external interface.
2. Use the SBC's name (and other information) to generate a *certificate request*.
3. Submit the certificate request to your local CA .
4. The CA will issue a signed certificate that contains the SBC's FQDN.
5. Load the device certificate into the SBC's Private Certificate Store.
6. Download a *Root certificate*, from the CA used to sign your certification request, in this case your local CA (Windows Local Domain Controller)

7. Load this Root certificate into the SBC's CA Certificate Store.

These numbered steps will be referenced in the instructions, below.

8.1.2 Creating a Certificate Request

In the SIParator web interface (Ingate Control Panel), select **Basic Configuration** > **Certificates**.

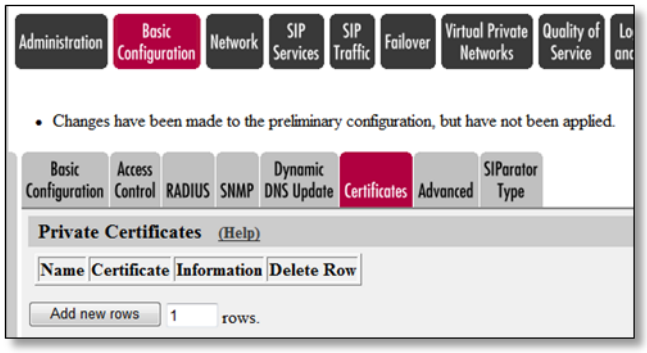


Figure 23. Navigation to private certificates

Under **Private Certificates**, enter **1** as the number of rows and click **Add New Rows**.

On the screen that appears next (Figure 24), enter an identifying **Name** (e.g. **SBC at HQ**) for the new certificate and click **Create New**.

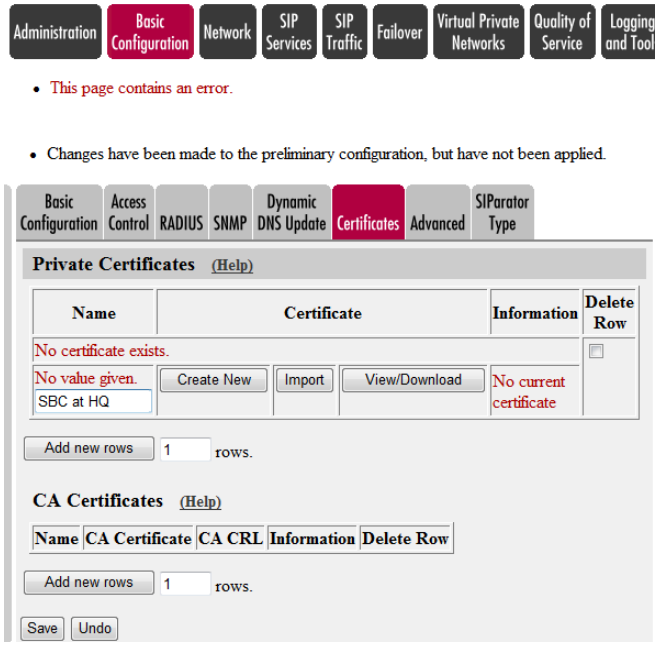


Figure 24. Adding a private certificate

Fill in the resulting **Create Certificate or Certificate Request** form (Figure 25) as described below.

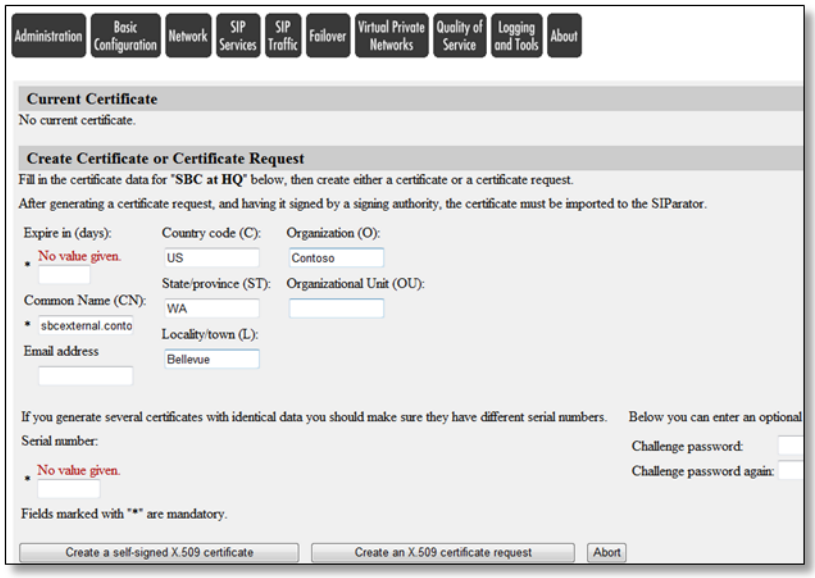


Figure 25. Certificate request details

Despite indications to the contrary[2], there is only one mandatory field for CA-signed certificate requests:

The *Common Name (CN)* field must contain the fully qualified domain name (FQDN) chosen for the DNS entry that specifies the address of the external interface of the SBC (e.g. `sbcexternal.contoso.com`). This is required by Lync, which compares the address from which inbound calls arrive with the value in the CN, and rejects them if a match is not found. This corresponds to **Step 1** under section **8.1.1 Configuring Certificates**.

There are also some optional fields, e.g.

- The *Country Code (C)* field should contain the two-letter country code[3] for your organization's location (e.g. US for United States, GB for United Kingdom, JP for Japan, etc.).
- The *Organization (O)* field should contain the name of your organization.
- Email address
- State/province (ST) and Locality/town (L) fields should contain location details
- Organizational Unit (OU) can contain other OUs or specific objects

When you have filled in the Common Name (and as many of the optional fields as desired), click the button labeled **Create an X.509 certificate request**. This corresponds to **Step 2** under section **8.1.1 Configuring Certificates**.

After a short pause, details of the certificate request will be displayed (Figure 26).

---

[2] If the *Serial Number* field is pre-populated with a value, leave this as it is. If it is empty, you do not need to provide a value.

[3] http://www.iso.org/iso/country_codes/iso_3166_code_lists/english_country_names_and_code_elements.htm

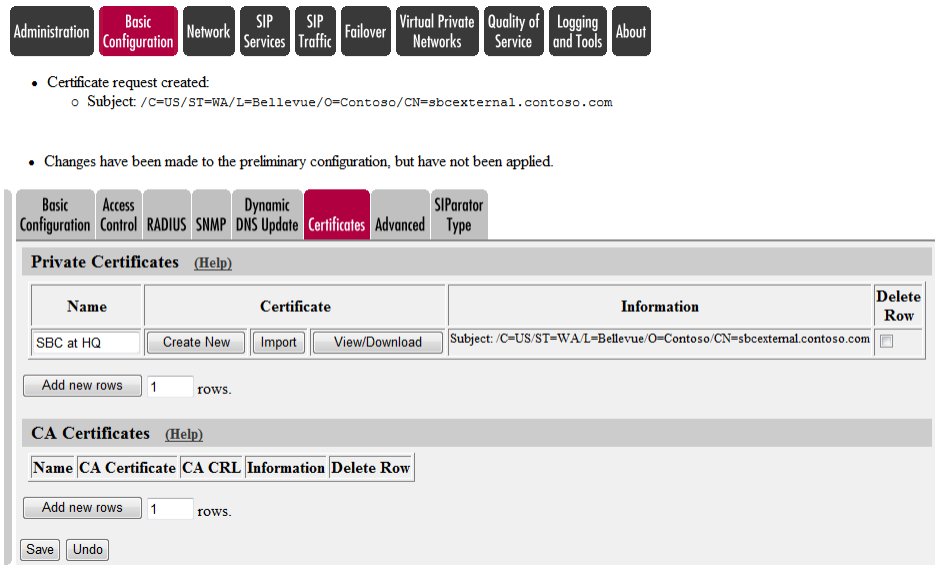


Figure 26. New certificate request

Examine of the details of the certificate request. Check that the subject name (CN) exactly matches the FQDN of the SBC.

If the information is correct, click the button labeled **View/Download**.

Figure 27. Viewing the certificate request

When the current certificate request is displayed (Figure 27), click the button labeled **Download certificate/certificate request (PEM format)**.

You will see a notification from your browser, asking if you want to open a file or save a file called `certreq.cer`. (DER Format)

Save the file somewhere convenient. If you open it in a text editor (e.g. Windows Notepad), it should look something[4] like this:

[4] Note that the actual content of your certificate request will be different because it contains information specific to your system.

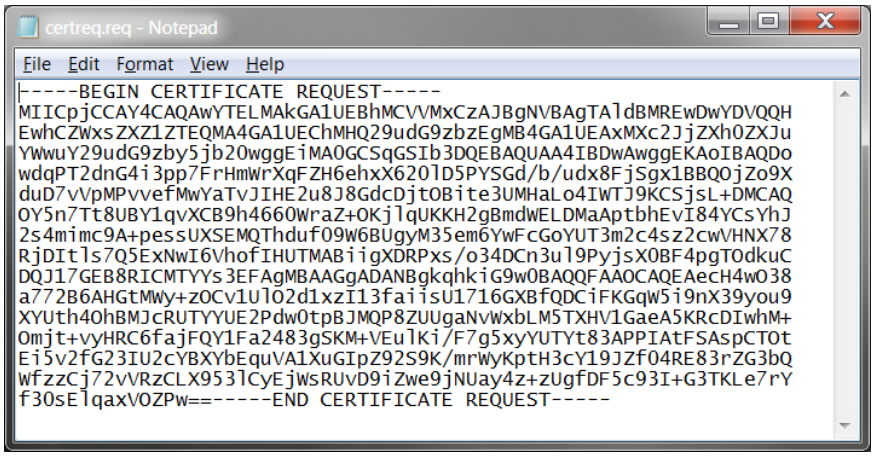


Figure 28. Certificate request as file

Use this certificate request as the input to your chosen Certificate Authority's process for generating and signing the certificate that you will use for this SBC Lync. This corresponds to **Step 3** under section 8.1.1 Configuring Certificates.

The process of generating and downloading a certificate varies from one CA to another: please consult the chosen CA's web site for details or Windows own CA in your local domain if used.

8.1.3 Importing an SBC Device CA-Signed Certificate

Download the certificate from the CA, saving it locally as a file. This corresponds to **Step 4** under section 8.1.1 Configuring Certificates.

Note: In the Ingate Release 5.0.5 or later, there is a direct import process for intermediate certificates. You must now import these Intermediate certificates into the Private Certificates store.

Place the file on the computer running the web browser that is being used to configure the SIParator (or in a place that is accessible to it).

Navigate to **Basic Configuration** > **Certificates**.

Under **Private Certificates**, select the entry corresponding to the **Certificate Request** that you made earlier.

Click on the button labeled **Import**.

Under *Import Signed Certificate* on the resulting screen (Figure 29), click on the **Browse…** button and navigate to the file that you downloaded.

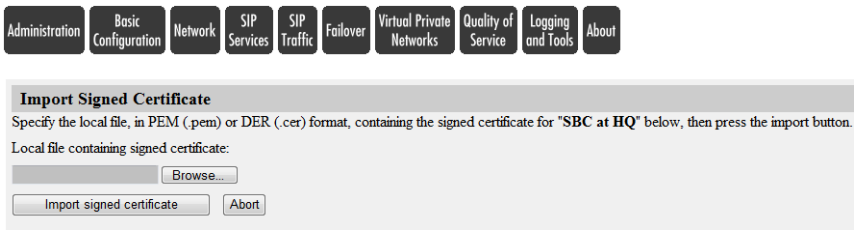


Figure 29. Preparing to import the CA-signed certificate

When you have selected the file, click the button labeled **Import signed certificate**. This corresponds to **Step 5** under section [8.1.1 Configuring Certificates](#).

There will be a brief pause while the SBC processes the certificate, and then it should be displayed.

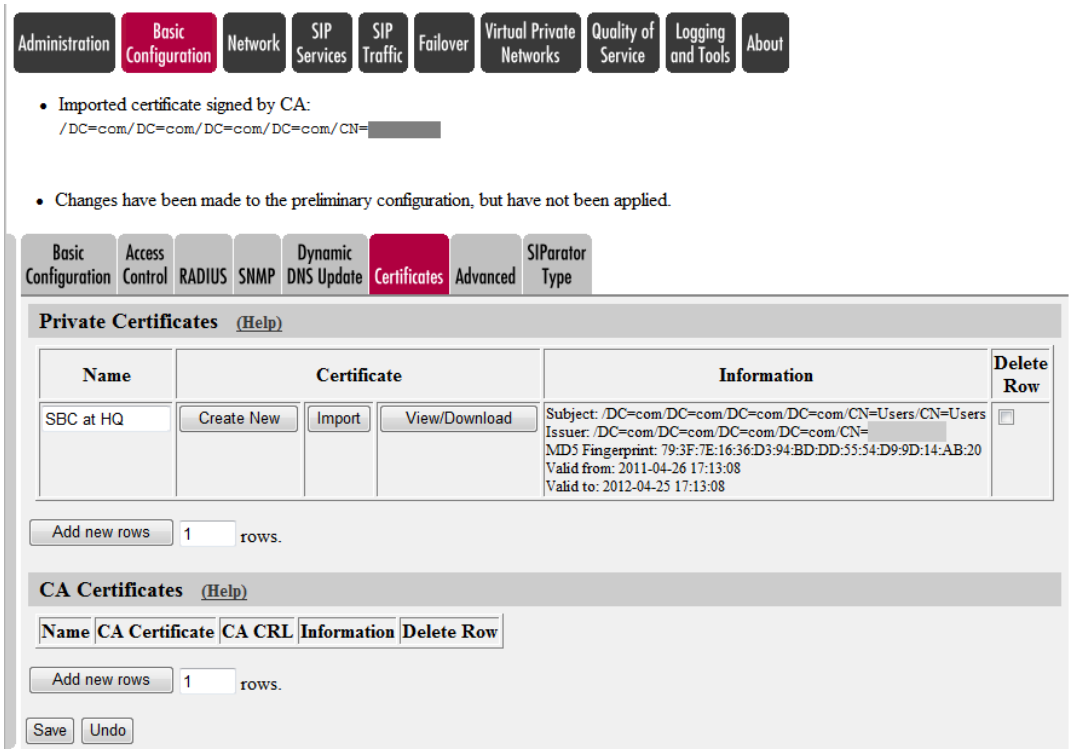


Figure 30. Certificate after import into the SIParator

Click on **Save** to apply the changes and store the certificate in the device's configuration data.

8.1.4 Importing Intermediate Certificates (if available)

Ingate software releases before version 4.10.2 combined the Intermediate and SBC Certificates prior importing. In Ingate release 4.10.2 direct import process was introduced, which is assumed. It is strongly recommended that you use the latest software version available (version 5.0.5 or higher).

You must now import these intermediate certificates into the Private Certificate store.

This is done after the SBC Device Certificate has been imported to the Ingate in Section: 8.1.3 Importing an SBC Device CA-Signed Certificate.

In the SIParator web GUI go to **Basic Configuration** > **Certificates**. Under **Private Certificates**, go to the section with the SBC Device Certificate. Under the **Certificate** column click **Import**.

On the screen that is displayed under **Import Intermediate Certificate**, click the **Choose File** button and then navigate to the file in which you saved the Combined SBC Device & Intermediate Certificate and select it.

Click on the button labeled **Import CA certificate**. This corresponds to **Step 6** under section [8.1.1 Configuring Certificates](#).

After a pause, details of the newly-imported certificate should be shown, along with those of the other certificates recently imported.

8.1.5 Importing a Root Certificate

Communication between the SBC and Lync will require mutual TLS. Not only will Lync authenticate the SBC (by means of the device certificate that you imported), but your SBC must also authenticate Lync. To allow the latter kind of authentication, you must ensure that your SBC is also loaded with a root certificate for the Certificate Authority that is used to sign the certificate that will be presented by the Microsoft Lync.

There are some options:

- Baltimore CyberTrust RootCA

To obtain this certificate, use a web browser to navigate to

https://www.cybertrust.ne.jp/SureServer/file/root_ca/BCTRoot.txt

- CTE CyberTrust Root CA

To obtain this certificate, use a web browser to navigate to
https://secure.omniroot.com/cacert/ct_root.der.

Figure 31: GTE CyberTrust Root Certificate

Copy and paste the text in to text editor (e.g. Windows Notepad), and save as a local file called `ct_root.cer`. This corresponds to **Step 7** under section **8.1.1 Configuring Certificates**.

Under **Basic Configuration** > **Certificates** in the Ingate control panel, under *CA Certificates*, click **Add new rows** to add 1 new row.

In the *Name* field of the new row, enter a descriptive name for the certificate (e.g. **LocalDomainRoot** or **CyberTrust Root**). Then, click the button (under the *CA Certificate* column) labeled **Change/View**.

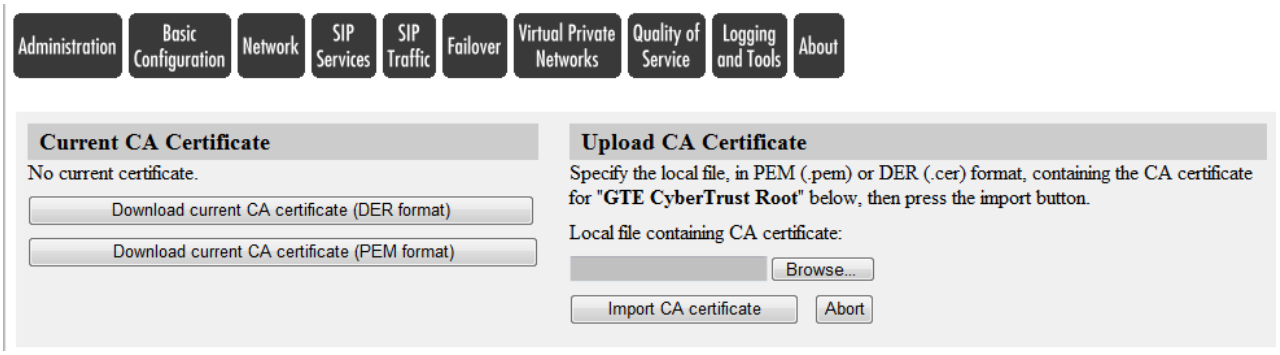


Figure 32. Preparing to import the root certificate

On the screen that is displayed (Figure 32), click the **Choose File** button and then navigate to the `ct_root.cer` file that you just saved, and select it.

When the file name is displayed under *Local file containing CA certificate*, click on the button labeled **Import CA certificate**. This corresponds to **Step 8** under section [8.1.1 Configuring Certificates](#).

After a pause, details of the newly-imported root certificate should be shown, along with those of your CA-signed device certificate (Figure 33).

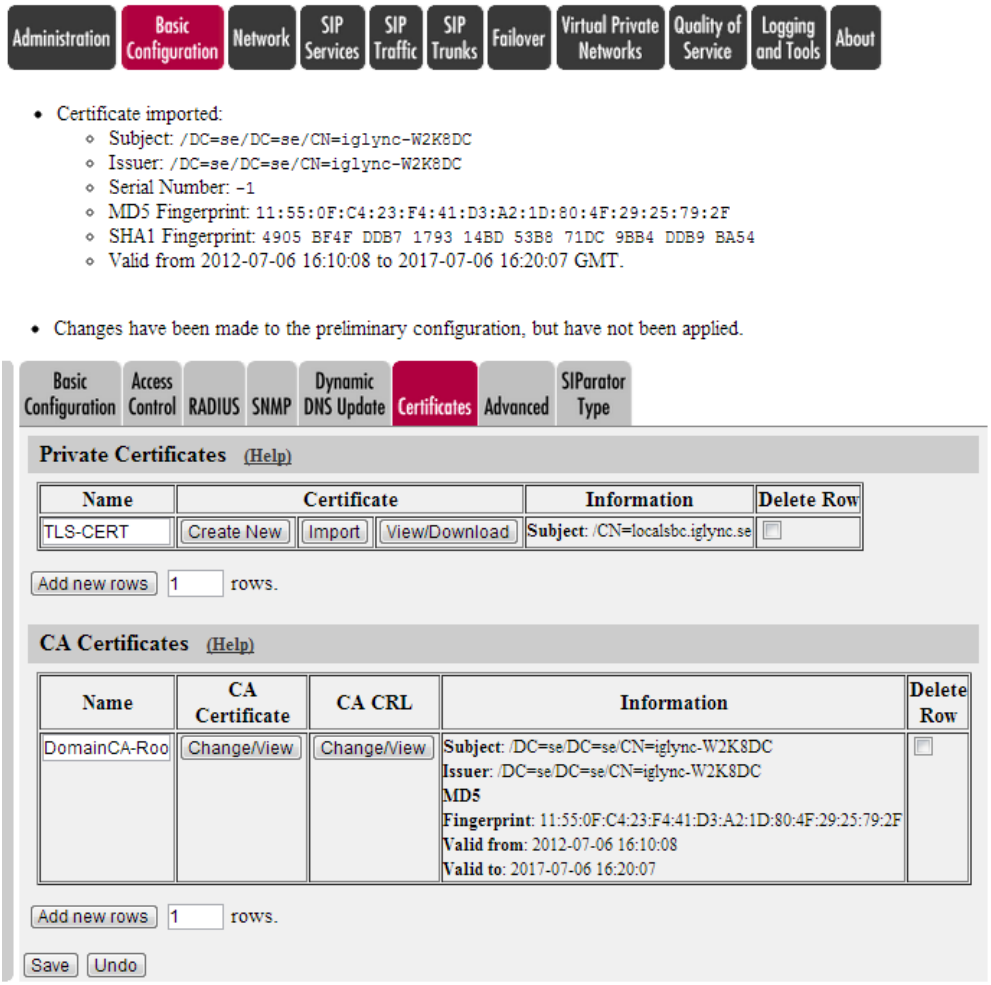


Figure 33. After importing the root certificate

Click on **Save** to save the certificate into the SBC's configuration data.

You will now refer to the certificates while configuring Transport Layer Security (TLS).

8.2 TLS Setup

Navigate to **SIP Services** > **Signaling Encryption** (Figure 34).

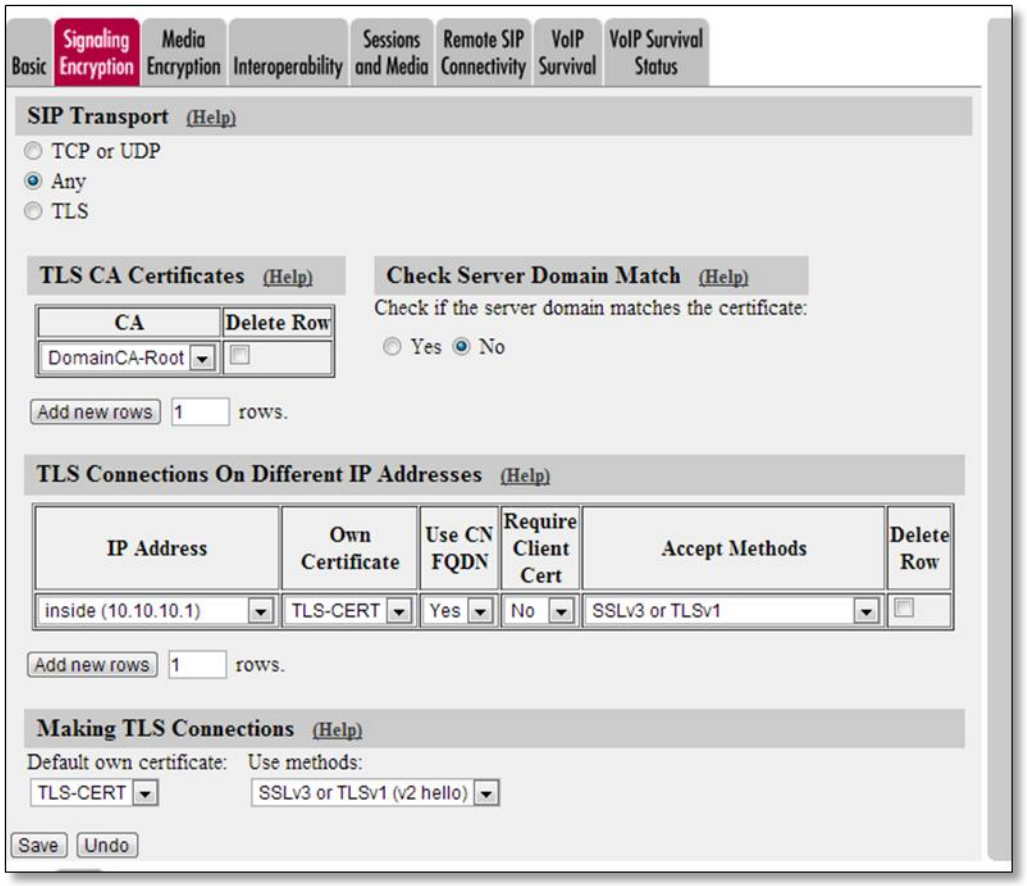


Figure 34. Configuring signaling encryption

Under **SIP Transport**, select **Any**.

Under **TLS CA Certificates**, select the root certificate that you imported earlier (*Importing a Root Certificate*, page 24).

Under **Check Server Domain Match**, select **No**.

Under **TLS Connections** on Different IP Addresses, configure as follows:

Set **IP Address** to that of the internal interface (see page 8).

Set **Own Certificate** to be the device certificate that you imported earlier

Set **Require Client Cert** to be **No**.

Set **Accept Methods** to be **Any**.

Under **Making TLS Connections**, configure as follows:

Set **Default own certificate** to be the device certificate that you imported earlier.

Set **Use methods** to be SSLv3 or TLSv1 (TLSv1 hello).

8.3 Configuring Media Encryption (SRTP)

Secure Real Time Protocol (SRTP) must be used to secure media (audio data) between the SIParator and Lync. However, you may use either RTP or SRTP between the VoIP Gateway (or IP PBX) and the internal interface of the SIParator. If you use RTP for internal media and SRTP for external media, you will need to create two "Crypto Suite Groups" (see below), one (cleartext) for the internal RTP traffic and another (ciphertext) for the external SRTP traffic. The directions below describe how to set this up[5].

Navigate to **SIP Services** > **Media Encryption**.

[5] If you decide to use SRTP for internal media traffic as well, you need only create a single Crypto Suite Group (ciphertext).

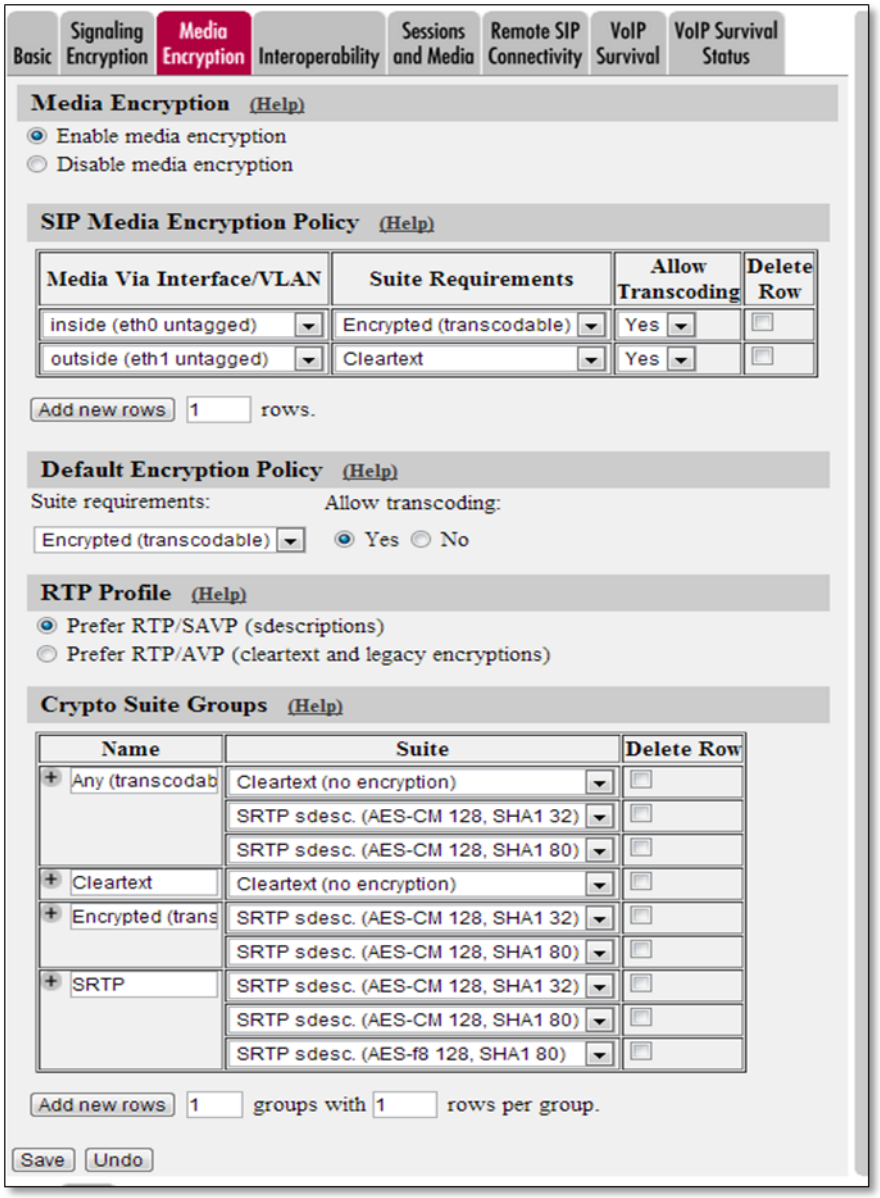


Figure 35. Configuring media encryption

Under **Media Encryption**, select **Enable media encryption**.

Under **Crypto Suite Groups** section, configure as follows:

Under **SIP Media Encryption Policy**, click **Add new rows**

Under **Media Via Interface/VLAN**, select the internal interface **(Eth0)**

Under **Suite Requirements**, select **Encrypted**

Under **Media Via Interface/VLAN**, add a new row and select the external interface **(Eth1)**

Under **Suite Requirements**, select **Cleartext**

Under **Default Encryption Policy section**, configure as follows:

Under **Suite Requirements**, select **Encrypted (transcodable)**

Under **Allow Transcoding**, select **Yes**

Under **RTP Profile**, select **Prefer RTP/SAVP** (**sdescriptions**)

Click **Save**.

8.4 Configuring Dial Plans

In the final stage of SIParator configuration, you need to force all traffic coming from mediation servers to be TLS

Navigate to **Configuration > SIP Traffic > Dial Plan.**

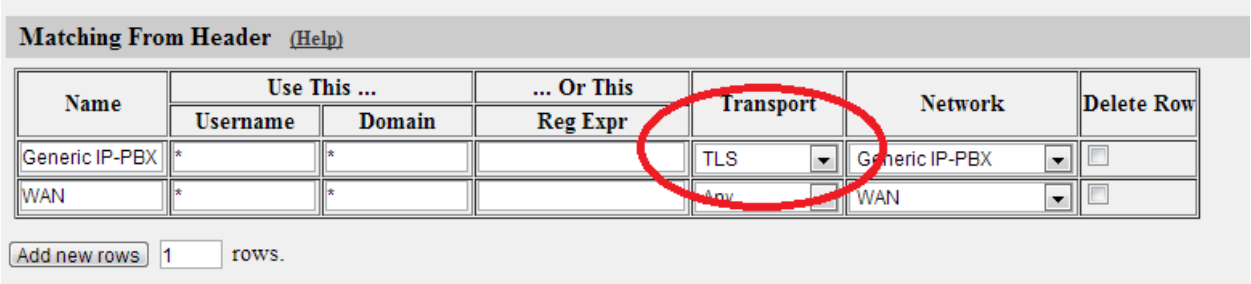


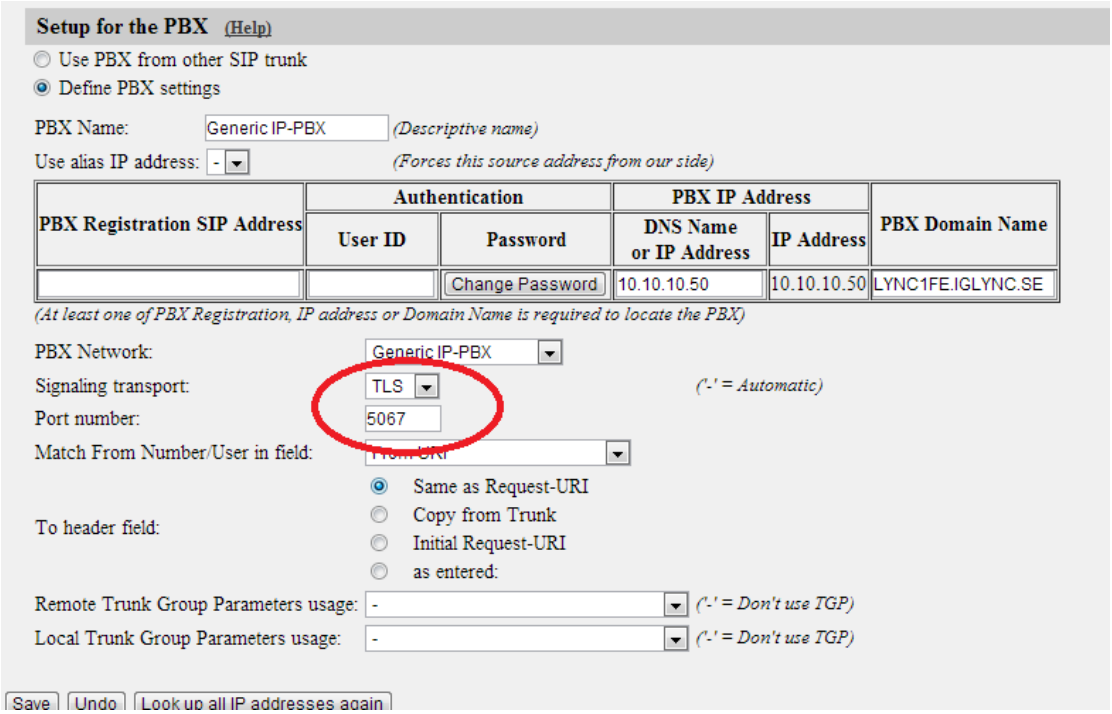
Figure 36. Configuring SIParator Dial Plans

Change the row "Generic IP-PBX" – Transport to **TLS**, this will force the SIParator to only accept TLS signaling.

8.5 Configuring SIP Trunk Page

In the final stage of SIParator configuration, you need to force all traffic coming from mediation servers to be TLS

Navigate to **Configuration > SIP Trunks > Trunk 1**.



Configuring SIParator Dial Plans

Change the **Signaling transport** to **TLS**. This will force the SIParator to send only TLS signaling to Lync server. You can change also to any port that Lync uses for TLS signaling.

Save and Apply the Configuration.

8.6 Using TLS and SRTP over the ITSP SIP Trunk

Some service providers (ITSPs) offer encrypted and extra secure connections on their SIP trunks. The Ingate SIParator fully supports such options and can also transcode between UDP/TCP/TLS used for signaling and RTP/SRTP for media, on either side of the SIParator.

Configuring TLS and SRTP towards the ITSP is very similar to sections 8.1to 8.4 above, but using the WAN interface (**Eth1**) instead of the LAN interface (**Eth0**). However, when coming to section 8.5 Configuring SIP Trunk Page, you should make the **TLS Signaling transport** in the **SIP Trunking Service** part at the top (rather than in the **Setup for the PBX** at the bottom.)