ingate

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

February 2015

Table of Content

1	Introduction	3
1.1	Before you Begin	3
1.2	Compatibility and Limitations	3
2	How an Ingate SIParator SBC fits into your Lync Deployment	4
3	Configuration Checklist	5
4	Step 1: Configure Lync to work with an E-SBC	6
5	Step 2: Set Up and Connect the SIParator	6
5.1	Hardware and Network Setup	6
5.2	Ingate Startup Tool (SUT)	7
5.2.1	First Time Setup of the SIParator	7
5.2.2	2 Network Topology	10
6	Step 3: The Initial Configuration of the SIParator	12
6.1	IP-PBX Configuration	12
6.2	ITSP Configuration	12
6.3	Uploading the Configuration	14
7	Administration Web GUI (Graphical User Interface)	15
7.1	Applying the Configuration	15
7.2	Additional Manual Configuration Using the Web GUI	17
7.2.1	The Lync Mediation Server on Another Subnet	18
8	Step 4: Optional TLS and SRTP Encryption and Using Certificates	18
8.1	Configuring TLS SIP Signaling Encryption	18
8.1.1	Configuring Certificates	18
8.1.2	Creating a Certificate Request	19
8.1.3	Importing an SBC Device CA-Signed Certificate	22
8.1.4	Importing Intermediate Certificates (if available)	23
8.1.5	Importing a Root Certificate	24
8.2	TLS Setup	26
8.3	Configuring Media Encryption (SRTP)	27
8.4	Configuring Dial Plans	29
8.5	Configuring SIP Trunk Page	29
8.6	Using TLS and SRTP over the ITSP SIP Trunk	30

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 <u>Microsoft's site</u>
- 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 Module¹

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: <u>http://www.ingate.com/Confirmed_ITSP.php</u> (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: <u>https://www.ingate.com/Confirmed_IP-PBX.php</u>

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





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 <u>Ingate documentation</u> 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 <u>Configuration Guide for</u> <u>Microsoft OCS 2007</u>

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 <u>http://www.ingate.com/Startup_Tool.php</u>. 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**.

Velcome to	o the Ingate Startup tool - this tool will assist you in setting up your	new Ingate unit
Setup		
	LAN	
	Connect your computer to your Ingate unit like this.	
Ingat	e model - Please Select model	
	Ingate Firewall/SIParator	
	Ingate Firewall/SIParator	
	SIParator SBE	

Figure 6. Device selection screen

You will see a configuration page (Figure 7).

	Help	
Version information is not available.		Help
Ingate Startup Tool TG- Helps configure your Ingate unit Ingate Startup Tool TG Version Version information is not available. First select what you would like to do: © Configure the unit for the first time © Change or update configuration of the unit © Check SIP configuration and logs Register this unit with Ingate © Lonfigure SIP trunking Backup the created configuration © Configure SIP trunking Backup the created configuration © Configure SIP trunking Backup the created configuration © Configure SIP trunking Salexup Ingate Startup Tool TG Version 1.0.7 Information about a newer version of this tool is not available. Could not connect to www.ingate.com No response from unit when trying to assign IP address with magic ping. Check your settings and cabling. The program field to assign an IP address to #10 Paled to contact the unit, check settings and cabling	ssword, establish contact	
Configure the unit for the first time Change or update configuration of the unit Check SIP configuration and logs Register this unit with Ingate Upgrade this unit Enable SIP module Configure Remote SIP Connectivity Configure SIP trunking Backup the created configuration Create a config without connecting to a unit This tool remembers passwords	Inside (Interface Eth) IP Address: MAC Address: Select a password Password: Confirm Password: Interface of your PC Ansilutning till	0) 10 , 10 , 10 , 1 00-90-fb-3d-29-fb okalt n_tverk
status		

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.

Inside (Interface Eth0)							
IP Address:	10	•	10	•	10	•	1
MAC Address:	00-90-fb-3d-29-f0						

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).

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

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).

Interfa	ce of your PC	
	Bluetooth Network Connection Local Area Connection Loopback Pseudo-Interface 1 Wireless Network Connection	

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.)

work Topology IP-PE	IX ITSP Upload Configuration
Product Type Inside (Internce E	Standalone SIParator th0)
IP address:	10 10 10 1
Netmask:	255 . 255 . 255 . 0

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)**.

-Outside (Interface	Eth1)						
Use DHCP to obtain IP							
IP Address:	193 . 180 . 23 . 56						
Netmask:	255 . 255 . 255 . 0						
Allow https acce	ess to web interface from Internet						

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.

rk Topology IP-	-PBX ITSP Upload Configuration		
Product Type:	Standalone SIParator 🔹	\frown	
Inside (Interface	Eth0)	Internet	
IP address:	10 . 10 . 10 . 1		/
Netmask:	255 . 255 . 255 . 0		
Outside (Interfac	ce Eth 1)		Existing firewall
Use DHCP to	obtain IP	Ingate SIParator	
IP Address:	193 . 180 . 23 . 56	LAN	
Netmask:	255 . 255 . 255 . 0		
Allow https a	ccess to web interface from Internet	IP.PBX	
Gateway:	193 . 180 . 23 . 1	n ton	
		DNS server Primary: 8 8 8 Secondary: 8 8 4 4	3
Status		DNS server Primary: 8 8 8 Secondary: 8 8 4 4	3
Status Ingate Startup 1	Tool TG Version 1.0.7, connected to:	DNS server 8 8 8 8 Primary: 8 8 8 4 4 Secondary: 8 8 4 4 Ingate Firewall 1210, IG-094-143-4019-1 1	8
Status Ingate Startup 1 VoIP Survival VPN QoS Enhanced Secu 50 (+50 unutiliz	Tool TG Version 1.0.7, connected to: rity red) SIT Traversal Licenses	DNS server 8 8 8 8 8 9 Secondary: (Optional) 8 8 4 4 4 Ingate Firewall 1210, IG-094-143-4019-1 1 1 1 1	8
Status Ingate Startup 1 VoIP Survival VPN QoS Enhanced Secu 100 SIP User Ro	Tool TG Version 1.0.7, connected to: rity ted) SIP Traversal Licenses egistration Licenses	DNS server 8 8 8 8 Primary: 8 8 8 4 4 Secondary: 8 8 4 4 Ingate Firewall 1210, IG-094-143-4019-1 1	8
Status Ingate Startup 1 VoIP Survival VPN Gos Enhanced Secu 50 (+50 unutiliz 100 SIP User Rd Software Versio	Tool TG Version 1.0.7, connected to: rity red) SIP Traversal Licenses egistration Licenses on: 4.10.0	B 8 8 8 Secondary: (Optional) 8 8 4 4 Ingate Firewall 1210, IG-094-143-4019-1	3 4
Status Ingate Startup 1 VoIP Survival VPN GoS Ernhanced Secu S0 (+50 unutiliz 100 SIP User Re Software Versio	Tool TG Version 1.0.7, connected to: rity ted) SIP Traversal Licenses egistration Licenses on: 4.10.0	B 8 8 8 8 Secondary: (Optional) 8 8 4 4 Ingate Firewall 1210, IG-094-143-4019-1	3 1 111
Status Ingate Startup 1 VoIP Survival VPN GoS Enhanced Secu 50 (+50 unutila 100 SIP User Rd Software Versic	Tool TG Version 1.0.7, connected to: rity red) SIP Traversal Licenses egistration Licenses on: 4.10.0	B 8 8 8 8 Secondary: 8 8 4 4 (Optional) 8 8 4 4	3 3 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

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.

1	vork Topology I	P-PBX	ITSP	Upload	Configurati
	-IP-PBX (should	be loca	ted on t	the LAN) -	
	Type:	Micro	psoft Ly	nc	
	IP Address:	10).1	0.10	. 50
	🔽 Lise doma	in name			
	SIP Domain	: sma	rtcomp.	com	

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.

Name: Airspring Airspring Airspring ATRT Bandwidth.com Bandwidth.com Bendwidth.com Bandwidth.com Bendwidth.com Provider address BroadVox (IP Only) IP Address: Cell IP Cell IP Ceneric (register) Generic (register all) Generic (register all) Generic (register all) Generic (register all) Goldline Authentication name: Advanced Level3 (Wholesale) Prefix to match Level3 (Wholesale) Is Prefix to addit PaeTec (P Only) PaeTec (P Only) Prefix: Telepacific Telepacific Telepacific Teles SP-anslutning v1 Teles SP-anslutning v2 Thinktel Windstream Windstream Xo Status Autex	ork Topology ID-DRV	TTSP 1 Upload Configuration		
Telia SIP-anslutning v1 Telia SIP-anslutning v2 Thinktel Windstream Virgin XO	Name: Provider address IP Address: Use domain nar Advanced Prefix to match Prefix: Prefix to add to Prefix:	ITSP_1 Upload Configuration Airspring Airspring AT&T Bandrel Bandrel Bandwidth.com Bell Canada BroadVox (IP Only) BroadVox (Register) Cell IP CV Lightpath 2.0 Generic (register all) Generic (register all) Generic (register all) Generic (rossing Global Crossing Global Crossing Global Crossing Goldline Level3 (Wholesale) Level3 (Wholesale) Is Microsoft Office 365 UM Nectar PaeTec (IP Only) PaeTec (Register) Spitfre Telepacific Telepacific Teletek	DID (start of range) (user name):	
-	Status	Telia SIP-anslutning v1 Telia SIP-anslutning v2 Thinktel Windstream Virgin XO		*

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.

Name:	Generic (no register)	•
		_

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

	Provider addre	SS	
	Domain:	proxy12.lev.com	
	🔽 Use doma	in name	
)1	:		
r	Provider address		
ſ	Provider address — IP Address:	123 . 123 . 123 . 123	

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).

Ingate Startup Tool	X
Network Topology IP-PBX ITSP_1 Upload Configuration	
Disclaimer and Self-Certified vendor, every possible configuration, combination and/or software version has not been tested. For technical assistance regarding end-to-end interoperability issues, please contact support@ingate.com.	Verbose Logging (SIP debug)
	Final step Clogon to web GUI and apply settings Apply settings directly using serial interface Backup the configuration Upload
Status Ingate Startup Tool Version 2.4.0, connected to: Ingate SI I0 SIP Traversal Licenses I0 SIP Traversal Licenses	Parator 19, IG-092-702-2122-0
Software Version: 4.6.2 Error: Please enter number, name and domain. Error: Please enter number, name and domain.	
	Help

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).

uccess 🛛 🔀
Your configuration has been updated. When you press OK you will be redirected to your browser. Please login and press "Apply Configuration" in the Admin menu of the Ingate web interface.
ОК

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).



Iministration Basic Configuration Network Rules and Relays	SIP Services	SIP Traffic	Failover	Virtual Private Networks	Quality of Service	Logging and Tools
Save/Load Show User Onfiguration Configuration Administration Upgrad	Table Look	Date and Time	Restart	Change Language		
Test Run and Apply Conf (Help) Duration of limited test mode: 30 seconds Apply configuration	Sh 0 0 0 1	ow Mes On every On the Sa Never	ssage A page we/Load	About Unap	plied Cha	anges
Backup (Help) The permanent configuration is not affected. Save to local file Load from local file	e L	ocal file: [Browse	
Save/Load CLI Command File (H The permanent configuration might be affected Save config to CLI file Load CLI file	e <u>ip)</u> I by load E Loo	ling a CL al file:	I file.		Browse	
Abort All Edits (Help) The permanent configuration is not affected. Abort all edits	Re The p	load Fa	t configu	Configuration tration is not affi figuration	on <u>(Help</u> fected.	2

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.

Administration	Basic Configuration	Network	Rules and Relays	SIP Services	SIP Traffic	Failover	Virtual Private Networks	Quality of Service	Logging and Tools	About
You are curre Continue tes	ently testing the sting button v	e prelimin vithin 30 s	ary config econds, or	the firev	ou mus vall will	t press ei revert to t	ther the Save of the normal pen	configurati manent con	on or the figuration.	
Save con	figuration	Contin	ue testing	Rev	ert					

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).

Name	Subgroup	Lower Li	mit	Upper (for IP r	Limit anges)	Interface/VI AN	Delete
Name	Subgroup	or IP Address	IP Address	DNS Name or IP Address	IP Address		Row
+ Generic (no regi		123.123.123.123	0.0.0.0		255.255.255.255	-	
Generic IP-PBX	- 🔽	10.10.10.00	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.

Networks and Computers

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		
O Disable SIP Trunk		
SID Trumbing Service (II-1-)		
SIF Trunking Service (Help)		
O Use parameters from other SIP trunk		
Offine SIP trunk parameters		
Service name:	Generic (no register)	(Descriptive name)
Service Provider Domain:	123 123 122 122	(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	
	Enternaise demain	

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**.

Administration Configu • This page conta • Changes have by	ic ration Net ins an erro	twork SIP Service or.	SIP Traffic Fa	ilover Virtue Ne	al Private tworks	Quality of Service een applie	Logging and Too
Basic Access Configuration Control	RADIUS S	Dynam NMP DNS Upd	ic ate Certificate	es Advanced	SIParator Type		
Private Certifi	cates <u>(</u>]	<u>Help)</u>					
Name		Cer	rtificate		Inform	nation]	Delete Row
No certificate exis	ts.						
No value given. SBC at HQ	Create	New	ort Viev	v/Download	No cu certific	irrent cate	
Add new rows	1 r	ows.					
CA Certificate	s <u>(Help)</u>						
Name CA Certif	icate CA	CRL Infor	mation Del	ete Row			
Add new rows	1 r	ows.					
Save Undo							

Figure 24. Adding a private certificate

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

Administration Basic Configuration	n Network SIP Services Tr	SIP Failover Virtual Private Quality of Logging About About Service and Tools	
Current Certificate	e		
No current certificate.			
Create Certificate	or Certificate Reg	uest	
Fill in the certificate data	for "SBC at HQ" below	w, then create either a certificate or a certificate request.	
After generating a certific	ate request, and having	it signed by a signing authority, the certificate must be imported t	o the SIParator.
Expire in (days):	Country code (C):	Organization (O):	
No value given.	US	Contoso	
	State/province (ST):	Organizational Unit (OU):	
Common Name (CN):	WA		
* sbcexternal.conto	Locality/town (L):		
Email address	Bellevue		
If you generate several o	ertificates with identical	data you should make sure they have different serial numbers	Below you can enter an ontional
Serial number:			Challense and an option
No subscribes			Challenge password:
* No value given.			Chauenge password again.
Fields marked with "*" a	re mandatory.		
Create a self-sign	ned X.509 certificate	Create an X.509 certificate request Abort	

Figure 25. Certificate request details

Despite indications to the contrary², 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 <u>8.1.1 Configuring Certificates</u>.

There are also some optional fields, e.g.

- The *Country Code (C)* field should contain the two-letter country code³ 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 <u>8.1.1 Configuring Certificates</u>.

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 <u>http://www.iso.org/iso/country_codes/iso_3166_code_lists/english_country_names_and_code_elemen_ts.htm</u>

Administration	Basic Configuration	Network	SIP Services	SIP Traffic	Failover	Virtual Private Networks	Quality of Service	Logging and Tools	About
----------------	------------------------	---------	-----------------	----------------	----------	-----------------------------	-----------------------	----------------------	-------

• Certificate request created: o Subject /C=US/SI=WA/L=Bellevue/O=Contoso/CN=sbcexternal.contoso.com

Changes have been made to the preliminary configuration, but have not been applied.

Basic Configuration	Access Control	RADIUS	SNMP	Dynamic DNS Update	Certificates	Advanced	SIParator Type								
Private C	ertific	ates	(Help)	1											
Name	Name Certificate Information											Delete Row			
SBC at HQ	Create New Import View/Dowr				Download	Subjec	: /C=US/ST=	=WA/L=B	ellevue/C	=Contoso	/CN=sbc	external.	.contoso.cor	n	
Add new ro	ows	1	rows												
CA Certif	ficates	6 <u>(Hel</u>	<u>p)</u>												
Name CA	Certif	icate C	A CR	L Informa	tion Delet	e Row									
Add new ro	ows	1	rows												
Save Undo	-														

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.

Administration	Basic Configuration	Network	SIP Services	SIP Traffic	Failover	Virtual Private Networks	Quality of Service	Logging and Tools	About
Current	Private Cei	rtificate	for "S	BC at	HQ"				Expo
Current cert	ificate request:								You car
• Subje	ct: /C=US/ST	=WA/L=B	ellevue	/0=Con	toso/CN	I=sbcexterna	l.contos	o.com	Export
	Download certi	ificate/cert	tificate red	quest (D	ER forma	t)			Export
	Download cert	ificate/cert	tificate red	quest (P	EM forma	t)			
Return	to certificate pa	age							



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 something⁴ like this:

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

📋 certreq.req - Notepad	
<u>File Edit Fo</u> rmat <u>V</u> iew <u>H</u> elp	
BEGIN CERTIFICATE REQUEST MIICpjCCAY4CAQAwYTELMAkGA1UEBhMCVVMxCzAJBgNVBAgTA1dBMREwDwYDVQQH EwhCZWxsZXIZTEQMA4GA1UEChMHQ29udG9zbzEgMB4GA1UEAxMXc2JjZXhOZXJu YWwY29udG9zby5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKA0IBAQDo wdqPT2dnG4i3pp7FrHmWrXqFZH6ehxX6201D5PYSGd/b/udx8FjSgx1BBQOjZo9X duD7vVpMPvvefMwYaTvJIHE2u8J8GdcDjtOBite3UMHaLo4IWTJ9KCSjsL+DMCAQ OY5n7Tt8UBY1qvXCB9h4660WraZ+OKj1qUKKH2gBmdWELDMAAptbhEvI84YCSYhJ 2s4mimc9A+pessUXSEMQThduf09W6BUgyM35em6YWFCGOYUT3m2C4sz2cwVHNX78 RjDIIS7Q5EXhWI6VhofIHUTMABiiqXDRPxs/o34DCn3u19PyjsX0BF4pgT0dkuC DQJ17GEB8RICMTYYs3EFAgMBAAGgADANBgkqhkiG9w0BAQQFAAOCAQEAecH4w038 a772B6AHGtMwy+z0Cv1U102d1xzI13faiisU1716GXBfQDCiFKGqW5i9nX39you9 XYUth40hBMJCRUTYYUE2Pdw0tpBJMQP8ZUUgaNvWxbLM5TXHV1GaeA5KRcDIwhM+ Omjt+vyHRC6fajFQY1Fa2483gSKM+VEu1Ki/F7g5xyYUTYt83APPIAtFSAspCT0t Ei5v2fG23IU2CYBXYbEquVA1XuGIp292S9K/mrWyKptH3cY19JZf04RE83rZG3bQ WfzzCj72vVRzCLX9531CyEjWsRUvD9iZwe9jNUay4z+zUgfDF5c93I+G3TKLe7rY f30sE1qaxV0ZPw==END CERTIFICATE REQUEST	^
	· ·

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 <u>8.1.1 Configuring Certificates</u>.

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 <u>8.1.1 Configuring Certificates</u>.

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

Administration Configu	sic Network SIP Services	SIP Traffic Failover Virtual P Netwo	rivate Quality of Logging rks Service and Tools About	
Changes have b	een made to the prelimina	u=	not been applied.	
Basic Access Configuration Control	RADIUS SNMP DNS Upda	e Certificates Advanced SI	Parator Type	
Private Certifi	cates (Help)			
Name	Cert	ificate	Information	Delete Row
SBC at HQ	Create New Impo	t View/Download	Subject: /DC=com/DC=com/DC=com/DC=com/CN=Users/CN=Users Issuer: /DC=com/DC=com/DC=com/CN= MD5 Fingerprint: 79:3F:7E:16:36:D3:94:BD:DD:55:54:D9:9D:14:AB:20 Valid for: 2011-04-26 17:13:08 Valid to: 2012-04-25 17:13:08	
Add new rows	1 rows.			
CA Certificate	es <u>(Help)</u>			
Name CA Certi Add new rows Add new rows	ficate CA CRL Inform	ation Delete Row		
Save Undo				

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 **<u>8.1.1 Configuring Certificates</u>**.

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 <u>https://secure.omniroot.com/cacert/ct_root.der.</u>



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 <u>8.1.1 Configuring</u> <u>Certificates</u>.

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**.

Administration Basic Configuration Network Services Traffic Failover N	ual Private Quality of Logging About Service and Tools
Current CA Certificate	Upload CA Certificate
No current certificate.	Specify the local file, in PEM (.pem) or DER (.cer) format, containing the CA certificate
Download current CA certificate (DER format)	for GIE Cyber I rust Root below, then press the import button.
Download current CA certificate (PEM format)	Local file containing CA certificate:
	Browse
	Import CA certificate Abort

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 <u>8.1.1</u> <u>Configuring Certificates</u>.

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

Administration	Basic Configuration	Network	SIP Services	SIP Traffic	SIP Trunks	Failover	Virtual Private Networks	Quality of Service	Logging and Tools	About
----------------	------------------------	---------	-----------------	----------------	---------------	----------	-----------------------------	-----------------------	----------------------	-------

- · Certificate imported:
 - Subject: /DC=se/DC=se/CN=iglync-W2K8DC
 - Issuer: /DC=se/DC=se/CN=iglync-W2K8DC
 - Serial Number: -1
 - MD5 Fingerprint: 11:55:0F:C4:23:F4:41:D3:A2:1D:80:4F:29:25:79:2F
 - SHA1 Fingerprint: 4905 BF4F DDB7 1793 14BD 53B8 71DC 9BB4 DDB9 BA54
 - Valid from 2012-07-06 16:10:08 to 2017-07-06 16:20:07 GMT.
- · Changes have been made to the preliminary configuration, but have not been applied.

Basic Configuration	Access Control	RADIUS	SNMP	Dynamic DNS Update	Certificates	Advanced	SIParator Type			
Private (Certifi	cates	(<u>Help)</u>							
Nam TLS-CER	ie T	Create	New	Certificat	e View/Down	load Sut	Infor ject: /CN=	mation localsbc.iglync.se	Delete Row	
Add new re	ows 1	ro	WS.							
CA Cert	CA Certificates (Help)									
Nam	ie	C. Certif	A ficate	CA CI	RL		I	nformation		Delete Row
Nam DomainC	A-Roo	C. Certif Change	A ficate e/View	CA CI Change/	RL View Issu MD Fing Vali Vali	ject: /DC=se er: /DC=se s erprint: 11 d from: 201 d to: 2017-1	In e/DC=se/C DC=se/CN :55:0F:C4: 2-07-06 16:20	nformation N=iglync-W2K8 (=iglync-W2K8D 23:F4:41:D3:A2: 5:10:08 0:07	DC C 1D:80:4F:29:25:79:1	Delete Row

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).

Signaling Basic Media Encryption Media Interoperability Sessions and Media Remote SIP Connectivity VoIP Survival VoIP Survival
SIP Transport (Help)
© TCP or UDP
Any
© ILS
TLS CA Certificates (Help) Check Server Domain Match (Help)
CA Delete Rem Check if the server domain matches the certificate:
DomainCA-Boot
Add new rows 1 rows.
TLS Connections On Different IP Addresses (Help)
IP Address Own Certificate FQDN Cert
inside (10.10.1) 💌 TLS-CERT 💌 Yes 💌 No 💌 SSLv3 or TLSv1 🔍 🗖
Add new rows 1 rows.
Making TLS Connections (Help)
Default own certificate: Use methods:
TLS-CERT V SSLv3 or TLSv1 (v2 hello)
Save Undo

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 up⁵.

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).

Signaling Medic Basic Encryption Encrypti	on Interoperability and Media Connectivity Survival Status								
Media Encryption (Help)									
Enable media ence	ryption								
Disable media enco	cryption								
SIP Media Encry	yption Policy (Help)								
Media Via Interfa	ace/VLAN Suite Requirements Allow Delete Transcoding Row								
inside (eth0 untagg	ged) 💌 Encrypted (transcodable) 💌 Yes 💌 🔲								
outside (eth1 untag	gged) 💌 Cleartext 💌 Yes 💌 🗖								
Add new rows	rows.	l							
Default Encrypti	on Policy (Help)								
Suite requirements:	Allow transcoding:								
Encrypted (transcod	lable) 💌 💿 Yes 🔘 No								
RTP Profile (He	ln)								
Prefer RTP/SAV	P (sdescriptions)								
Prefer RTP/AVP	(cleartext and legacy encryptions)								
Crypto Suite Gro	oups (Help)	I.							
Name	Suite Delete Row								
🛨 Any (transcodab	Cleartext (no encryption)								
	SRTP sdesc. (AES-CM 128, SHA1 32) 💌 🔲								
	SRTP sdesc. (AES-CM 128, SHA1 80) 💌 🔲								
Cleartext	Cleartext (no encryption)								
Encrypted (trans	SRTP sdesc. (AES-CM 128, SHA1 32) 💌 🔲								
	SRTP sdesc. (AES-CM 128, SHA1 80)								
* SRTP	* SRTP SRTP Sdesc. (AES-CM 128, SHA1 32) -								
	SRTP sdesc. (AES-CM 128, SHA1 80)								
	SRTP sdesc. (AES-f8 128, SHA1 80) 💽 🔲								
Add new rows 1	groups with 1 rows per group.								

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.**

Matching From Header (Help)									
Nama	Use T	his Or This					Notwork		Dalata Dar
Name	Username	Domain	Reg Expr		Transport		Network		Delete Kow
Generic IP-PBX	*	*			TLS 🔻	G	heric IP-PBX	•	
WAN	*	*			Any	W	AN	-	
			<u> </u>						

Add new rows 1 rows.

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**.

Setup for the PBX (Help)								
O Use PBX from other SIP trunk								
Define PBX settings								
PBX Name: Generic IP-PBX (Descriptive name)								
Use alias IP address: 🛛 💌	(Force	es this source address j	from our side)					
	Auth	entication	PBX IP Ad	ldress				
PBX Registration SIP Address	User ID	Password	DNS Name or IP Address	IP Address	PBX Domain Name			
		Change Password	10.10.10.50	10.10.10.50	LYNC1FE.IGLYNC.SE			
(At least one of PBX Registration, I	P address or Dom	ain Name is required t	o locate the PBX)					
PBX Network:	Generic	IP-PBX						
Signaling transport:	TLS 💌		('-' = Au	tomatic)				
Port number:	5067							
Match From Number/User in field	: Trom Of		•					
	Sat	me as Request-URI						
To header field:	Co	py from Trunk						
10 100000 1000	Init	tial Request-URI						
	⊘ as	entered:						
Remote Trunk Group Parameters	usage: -		▼ ('-' = Do	n't use TGP)				
Local Trunk Group Parameters us	sage: -		▼ ('-' = Do.	n't use TGP)				

Save Undo Look up all IP addresses again

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.)