Configuration Guide

Ingate® SIParator®/Firewall E-SBC with Microsoft® Office 365 Unified Messaging (UM)

May 2015

Table of Contents

Terminology used in this document:

Abbreviation	Term
UM	Unified Messaging
SBC	Session Border Controller
CA	Certificate Authority
CR	Certificate Request
PBX	Public Branch Exchange
SUT(-TG)	Start Up Tool (– Trunk Groups)

Revision History:

Revision	Date	Author	Comments
	2012-06-21	MS, SB, KES	First published version
15B	2015-02-28	PD, RN, KES	Recreated + Updates
15C	2015-05-22	PD, AG	Minor TLS Fix

1 Introduction

This document describes how to configure Ingate's SIParator devices to work as Session Border Controllers for connecting to Office 365 Exchange Unified Messaging.

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, see Plan for UM.
- Current Ingate SIParator software (5.0.5 or later). Office 365 compliance was introduced with version 4.9.2, but only instructions for versions >= 4.10.1 are within this guide. Upgrading to the latest Ingate software is strongly recommended.
- Ingate SIParator SIP Trunking Module[1]

From Microsoft:

- Office 365 for Enterprises, with a service plan that includes UM.

1.2 Compatibilities and Limitations

The Ingate SIParator is among the Session Border Controllers (SBCs) that have been successfully tested for interoperability with Exchange Online. See: Session Border Controllers Tested with Exchange Online UM. The Ingate SIParator SBC has been tested to work with Office 365 UM, and the following PBXs and VoIP gateways:

- VoIP Gateway
- Dialogic DMG1000
- IP-PBX
- Cisco Unified Communications Manager

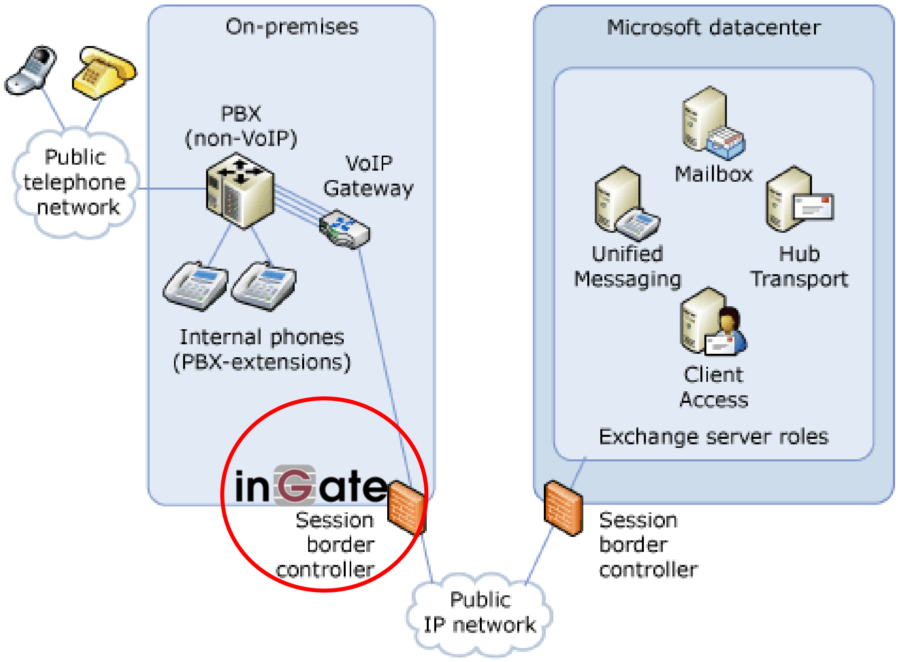
Ingate has confirmed Interoperability with IP-PBXs and VoIP Gateways independently for the use of SIP Trunking and other SIP applications, see the IP-PBX listing of Ingate. Even though all these combinations have not been individually lab tested specifically with the Microsoft Office 365 UM solution, many installations with the Microsoft Office 365 UM has successfully been done.

PBXs and VoIP gateways that have been tested with Exchange 2013 UM are listed at the Telephony Advisor for Exchange 2013 (and linked content).

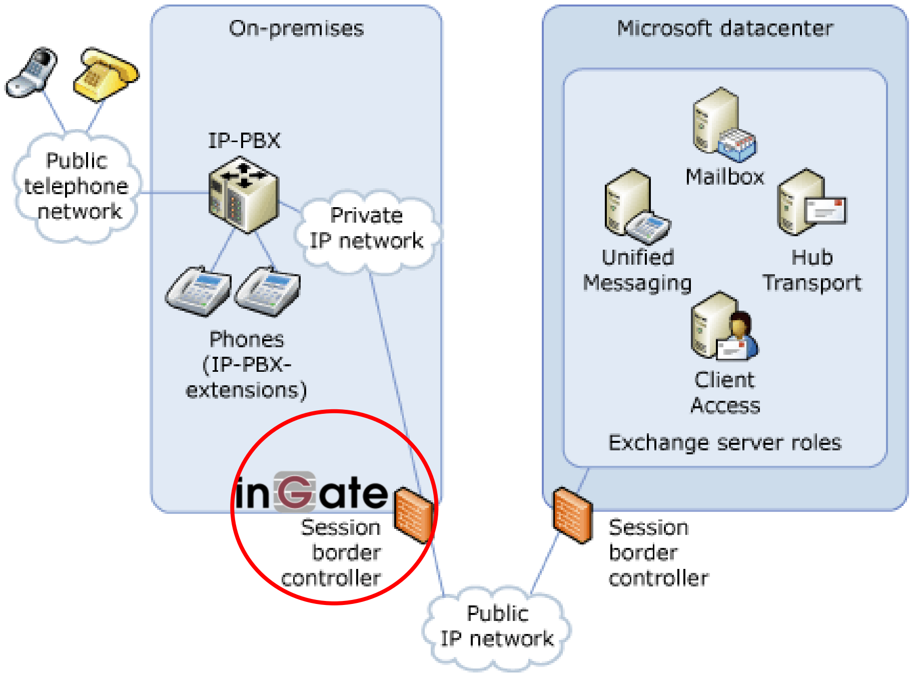
[1] The Ingate SIParator Enhanced Security module is also required, but is automatically included with recent versions of the SIParator/Firewall software. You can check that the Enhanced Security is included under the **About** tab in the administration GUI.

2 How an Ingate SIParator SBC fits into your UM deployment

If you have a PBX that doesn't support direct SIP communication with UM, thus requires a VoIP gateway between the PBX and UM, see Checklist: Connect a Traditional PBX to Exchange Online UM.



If you have an IP-PBX that supports direct SIP communication with UM, see Checklist: Connect an IP PBX to Exchange Online UM.



3 Configuration Checklist

You will need to complete the following steps in order to configure an Ingate SIParator session border controller (SBC) and Office 365 UM to work together. You need to configure DNS and UM first, and then configure the SBC to route traffic to and from Office 365 UM.

- Configure Office 365 Unified Messaging to work with a Session Border Controller
- Connect to the SBC and do Initial Configuration of the SBC
- Set SBC Options to work with Office 365 UM
- Verify SBC Configuration

This document describes the simplest SIParator configuration that will work with Office 365 UM. It assumes that you have one SIParator unit, and one IP PBX or VoIP gateway. If you have more complex requirements (e.g. multiple IP PBXs behind one SIParator, or multiple SIParators for high availability), please consult the Ingate documentation for details (login to your Ingate account is required).

4 Configure Office 365 UM to work with an SBC

Detailed information for this step is available here: Configuration Checklist: Configure Office 365 Unified Messaging to work with a Session Border Controller.

5 Connect to the SBC and do Initial Configuration of the SBC

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 TG (see below).

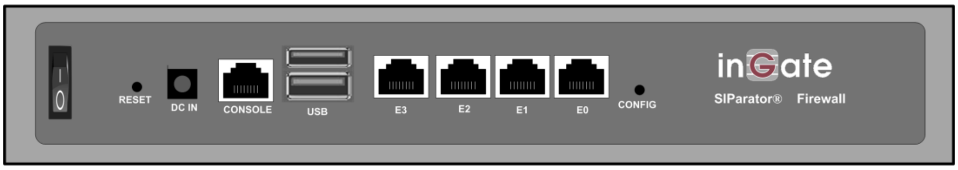


Figure 1. Back panel of Ingate SIParator 21

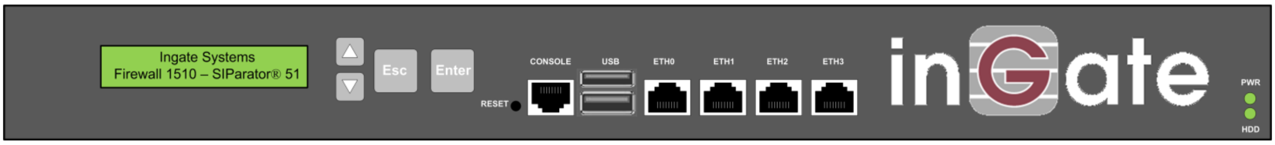


Figure 2. Front panel of Ingate SIParator 51, 56, 66

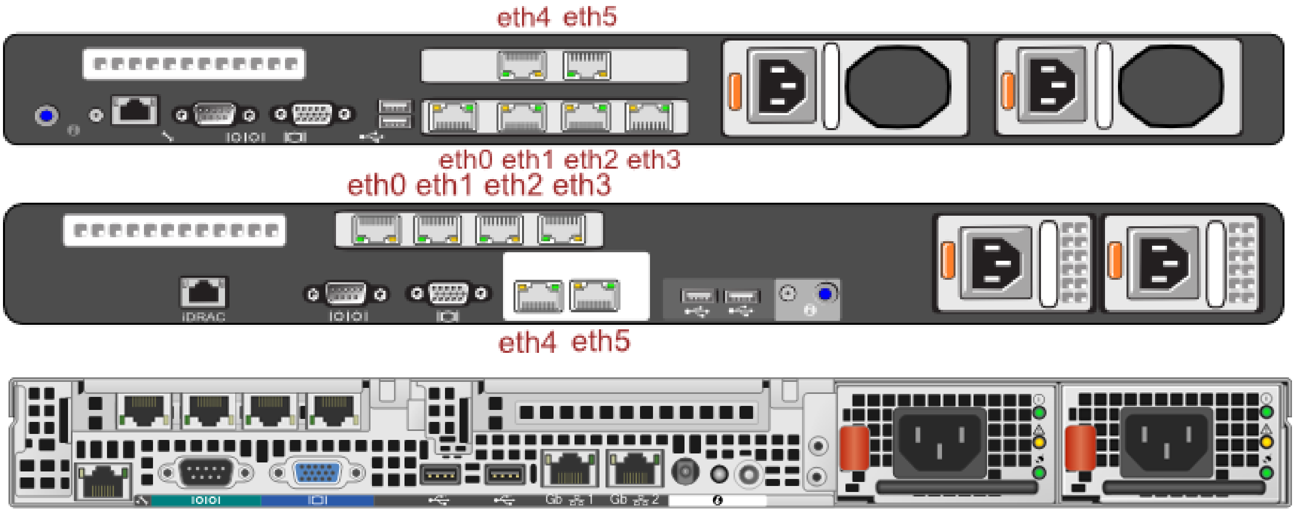


Figure 3. Back panel of Ingate SIParator 95, 96, 97, 98

The Ingate Startup Tool TG is an “Out-of-the-Box” commissioning tool and is not a “Config-Everything” tool, so it assumes some very basic networking topology and has some 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 TG assumes that **all of the following are connected to the same subnet on the private IP network**:

- SIParator (via port Eth0)
- VoIP Gateway or IP PBX
- Computer running the Ingate Startup Tool TG

If, for some reason, this is not the case (e.g. the VoIP Gateway or IP PBX is on a different subnet from the SIParator), the Startup Tool TG 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.

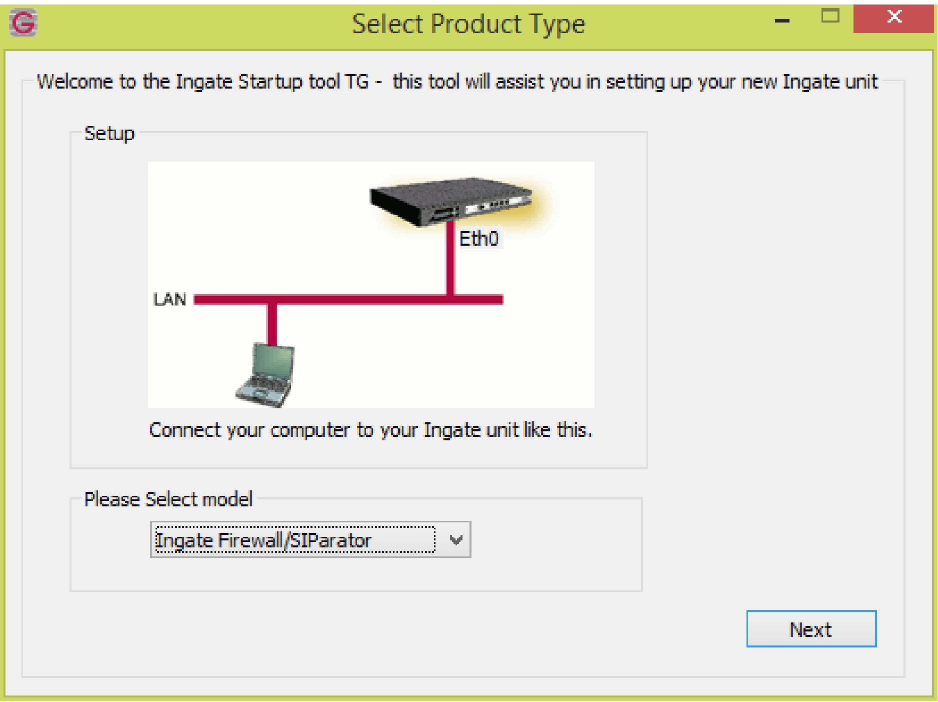
5.2 Ingate Startup Tool (SUT)

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 TG. 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_TG.php. Always use the latest version. 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.)

Launch the tool.



Select Product Type

Welcome to the Ingate Startup tool TG - this tool will assist you in setting up your new Ingate unit

Setup

Connect your computer to your Ingate unit like this.

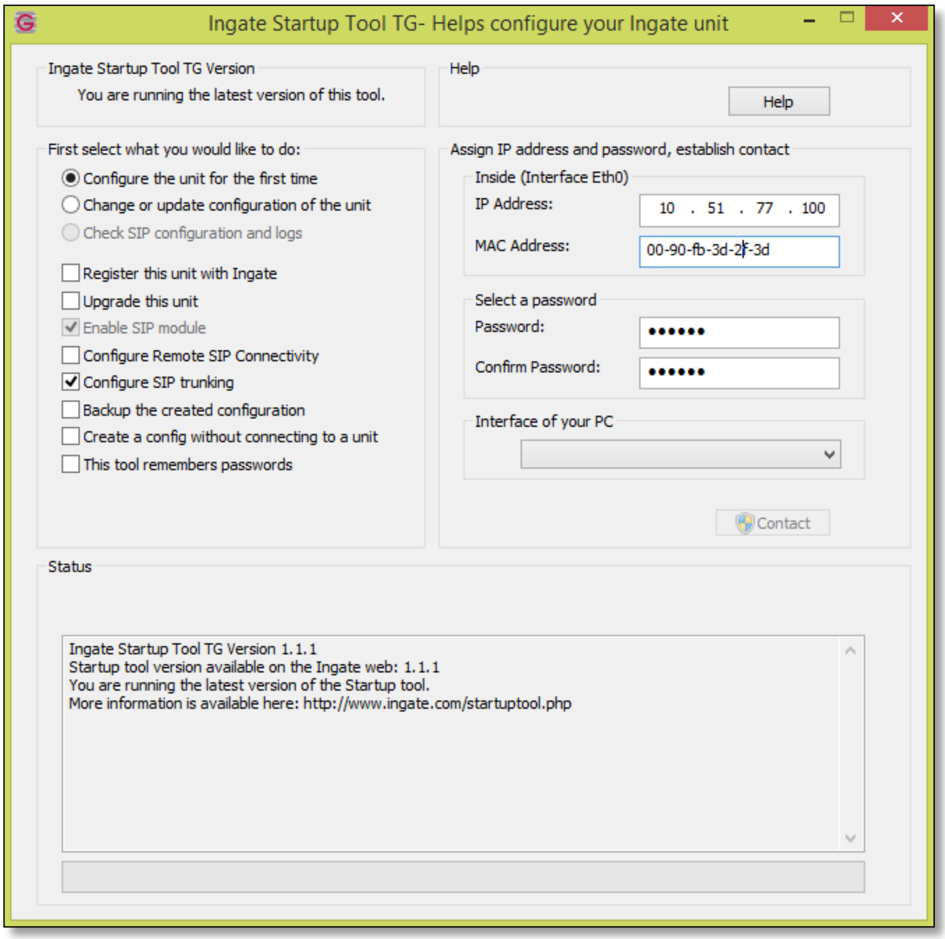
Please Select model

Ingate Firewall/SIParator

Figure 4. Product Type selection Screen

Select the model type of the Ingate unit as Ingate Firewall/SIParator (Figure 4) and click Next.

You will see a configuration page (Figure 5).



Ingate Startup Tool TG- Helps configure your Ingate unit

Ingate Startup Tool TG Version

You are running the latest version of this tool.

Help

First select what you would like to do:

- ● Configure the unit for the first time
- ○ Change or update configuration of the unit
- ○ Check SIP configuration and logs
- □ Register this unit with Ingate
- □ Upgrade this unit
- ☑ Enable SIP module
- □ Configure Remote SIP Connectivity
- ☑ Configure SIP trunking
- □ Backup the created configuration
- □ Create a config without connecting to a unit
- □ This tool remembers passwords

Assign IP address and password, establish contact

Inside (Interface Eth0)

IP Address: 10 . 51 . 77 . 100

MAC Address: 00-90-fb-3d-2f-3d

Select a password

Password: ••••••

Confirm Password: ••••••

Interface of your PC

Status

```
Ingate Startup Tool TG Version 1.1.1
Startup tool version available on the Ingate web: 1.1.1
You are running the latest version of the Startup tool.
More information is available here: http://www.ingate.com/startuptool.php
```

Figure 5. 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 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 5) shows an example.

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

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 6).

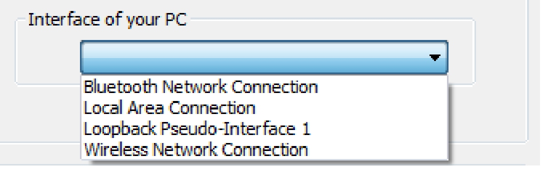

Interface of your PC
Bluetooth Network Connection
Local Area Connection
Loopback Pseudo-Interface 1
Wireless Network Connection

Figure 6. Selecting the network interface used by the Startup Tool TG

When these values have been entered, the **Contact** button at the bottom right of the form (Figure 5) will become active.

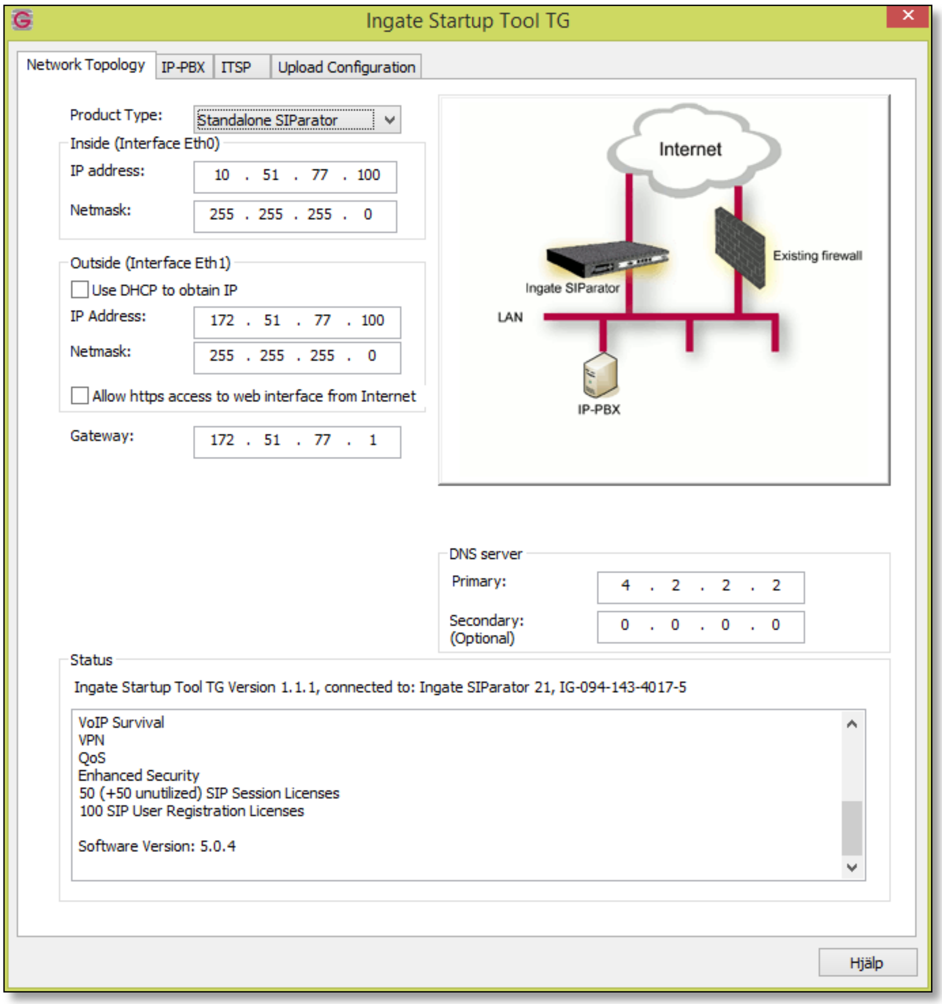
Press the **Contact** button.

The Startup Tool TG will find the Ingate unit on the network, 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.



Product Type: Standalone SIParator

Inside (Interface Eth0)

IP address: 10 . 51 . 77 . 100

Netmask: 255 . 255 . 255 . 0

Outside (Interface Eth1)

□ Use DHCP to obtain IP

IP Address: 172 . 51 . 77 . 100

Netmask: 255 . 255 . 255 . 0

□ Allow https access to web interface from Internet

Gateway: 172 . 51 . 77 . 1

DNS server

Primary: 4 . 2 . 2 . 2

Secondary: (Optional) 0 . 0 . 0 . 0

Status

Ingate Startup Tool TG Version 1.1.1, connected to: Ingate SIParator 21, IG-094-143-4017-5

VoIP Survival
VPN
QoS
Enhanced Security
50 (+50 unutilized) SIP Session Licenses
100 SIP User Registration Licenses

Software Version: 5.0.4

Figure 7. Configuring Network Topology

In the *Product Type* drop down list, select **Standalone SIParator** (Figure 7) if your network topology is as indicated by the picture to the right of the list. 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.)

After configuring the product type, the controls on the administrative interface will change, according to the type selected.

The internal network interface details, listed 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)*.

Once you have entered the internal and external interface details, go to the *Gateway* control and enter the address of the router that acts as a firewall gateway for your network.

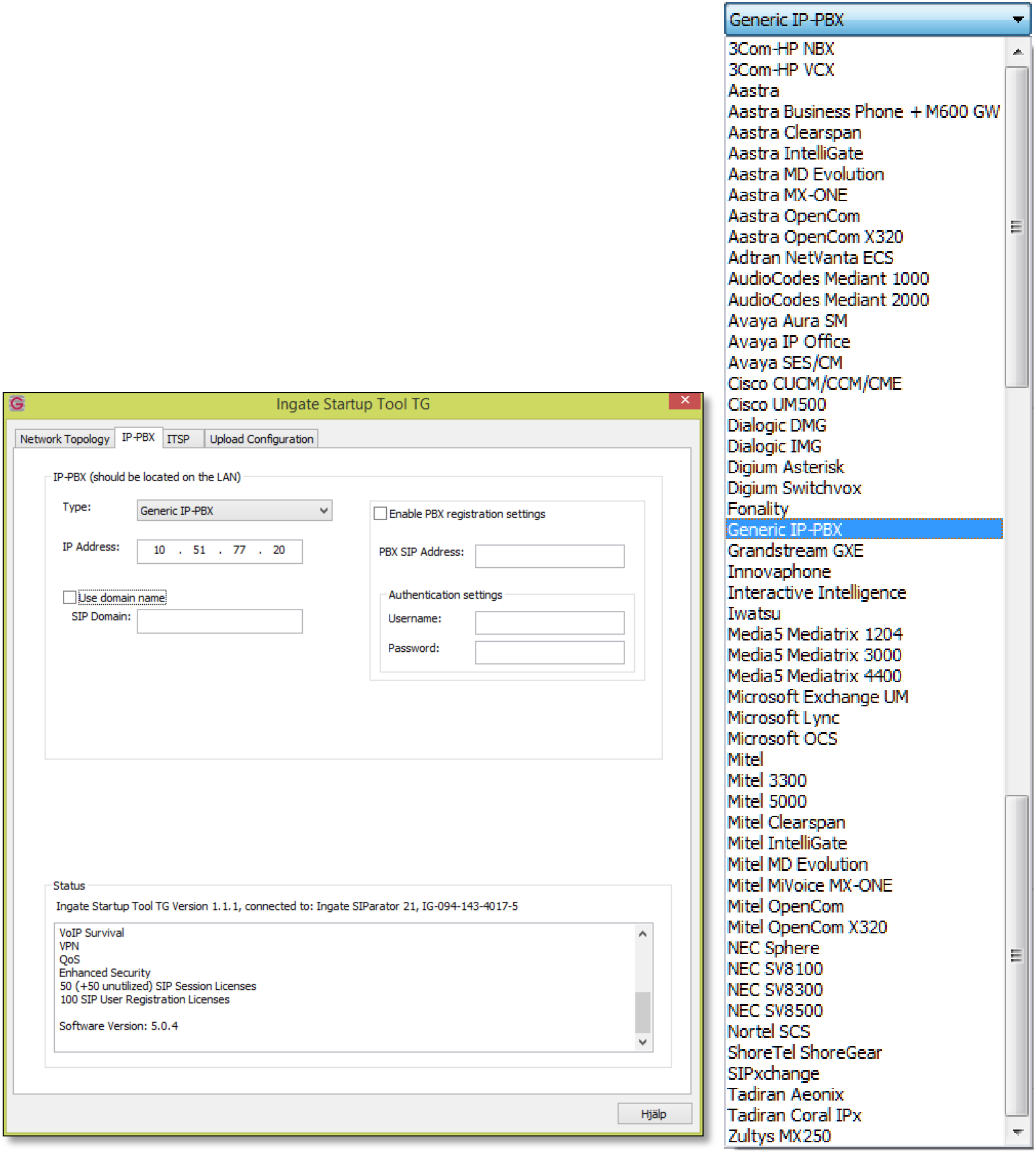
Finally, enter the DNS server IP addresses. These can be internal or external.

5.2.3 IP-PBX Configuration

Even though Office 365 UM is not acting as a telephony provider (dial tone is provided by your PBX or IP-PBX), there are configuration options that you need to set for your SBC to work with Office 365 UM.

In the Ingate Startup Tool TG, navigate to the *IP-PBX* tab (Figure 8).

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



Ingate Startup Tool TG

IP-PBX (should be located on the LAN)

Type: Generic IP-PBX

IP Address: 10 . 51 . 77 . 20

□ Use domain name

SIP Domain:

□ Enable PBX registration settings

PBX SIP Address:

Authentication settings

Username:

Password:

Status

Ingate Startup Tool TG Version 1.1.1, connected to: Ingate SIParator 21, IG-094-143-4017-5

```
VoIP Survival
VPN
QoS
Enhanced Security
50 (+50 unutilized) SIP Session Licenses
100 SIP User Registration Licenses

Software Version: 5.0.4
```

Figure 8. Configuring the IP PBX or VoIP Gateway details

In the *Type* drop-down list, select an entry that matches your IP PBX or VoIP Gateway. If you cannot find a matching item, select **Generic PBX**.

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

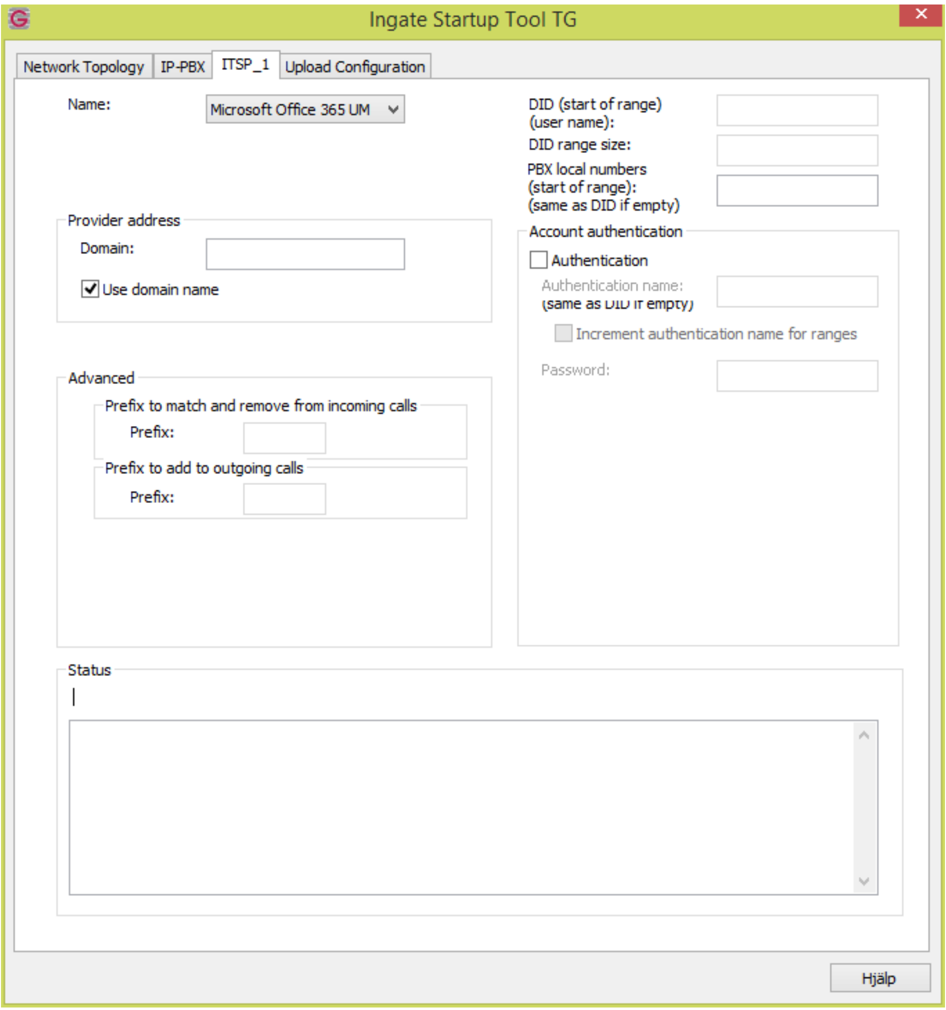
If the IP-PBX is behind another router on the LAN-side, you may have to set a local dummy IP address, not to be blocked by the Startup Tool and later, in the Ingate administration web GUI, change it and also add a static route to the Ingate E-SBC routing table. Consult the Ingate Reference Manual (Chapter 6 – Interface: Static Routing) for additional network setup (adding a static route).

5.2.4 ITSP Configuration

In the Ingate Startup Tool TG, navigate to the *ITSP* tab (Figure 9).

This configuration is related to the SBC's connection, via its external interface, to Office 365 Exchange UM.

ITSP stands for Internet Telephony Service Provider. However, Exchange UM is not acting as a telephony provider but it has the IP-PBX in the other of the SIP trunk.



Ingate Startup Tool TG

Network Topology | IP-PBX | ITSP_1 | Upload Configuration

Name: Microsoft Office 365 UM

Provider address
Domain:
☑ Use domain name

Advanced
Prefix to match and remove from incoming calls
Prefix:
Prefix to add to outgoing calls
Prefix:

DID (start of range) (user name):
DID range size:
PBX local numbers (start of range): (same as DID if empty)

Account authentication
□ Authentication
Authentication name: (same as DID if empty)
□ Increment authentication name for ranges
Password:

Status

Figure 9. Configuring the external SIP interface details

In the *Name* drop-down list, select **Microsoft Office365**.

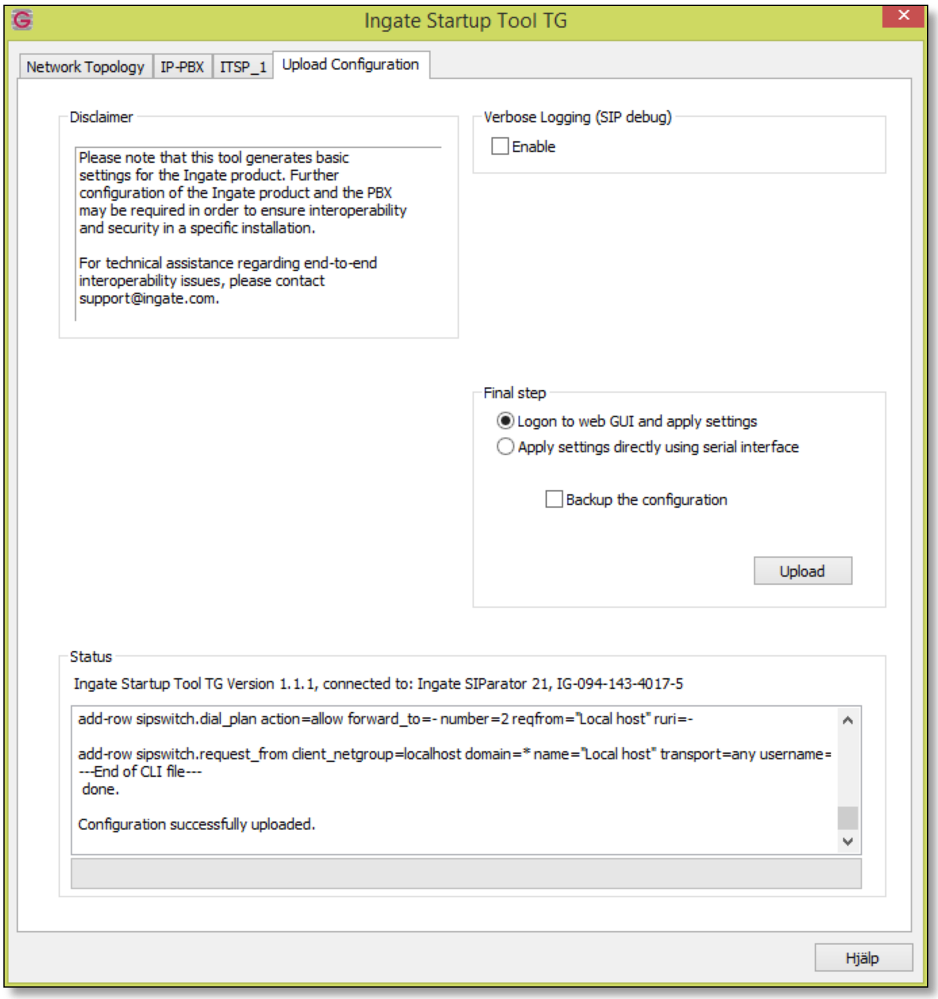
In the *Provider address* group box, check the box labeled *Use domain name*.

In the *Domain* field, enter the Forwarding Address (for example: **`7344b2b0-20e6-4332-9f5b-b508f7306ac1.um.outlook.com`**) that was assigned to the UM IP Gateway object that you created in the Exchange Online UM configuration for your UM Dial Plan (See: 4 Configure Office 365 UM to work with an SBC).

5.2.5 Uploading the Configuration

When you have completed the previous configuration steps, use the StartUp Tool TG to load the 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 10).



Ingate Startup Tool TG

Disclaimer

Please note that this tool generates basic settings for the Ingate product. Further configuration of the Ingate product and the PBX may be required in order to ensure interoperability and security in a specific installation.

For technical assistance regarding end-to-end interoperability issues, please contact support@ingate.com.

Verbose Logging (SIP debug)

□ Enable

Final step

● Logon to web GUI and apply settings

○ Apply settings directly using serial interface

□ Backup the configuration

Status

Ingate Startup Tool TG Version 1.1.1, connected to: Ingate SIParator 21, IG-094-143-4017-5

```
add-row sipswitch.dial_plan action=allow forward_to=- number=2 reqfrom="Local host" ruri=-

add-row sipswitch.request_from client_netgroup=localhost domain=* name="Local host" transport=any username=
---End of CLI file---
 done.

Configuration successfully uploaded.
```

Figure 10. Uploading configuration data to the SIParator

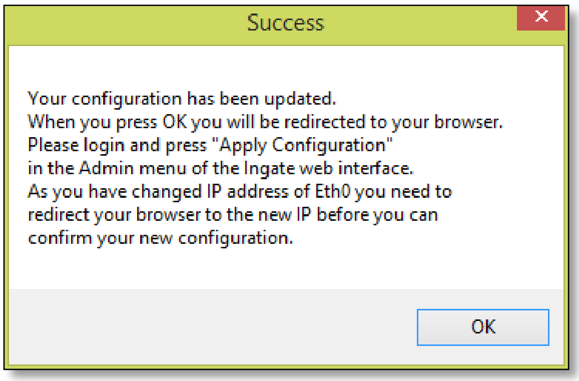
In the *Final step* controls, ensure that the radio button labeled *Logon to web GUI and apply settings* is selected.

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 TG to the SIParator.

When the data has been uploaded, a dialog box will appear (Figure 11).



Success

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.
As you have changed IP address of Eth0 you need to
redirect your browser to the new IP before you can
confirm your new configuration.

Figure 11. Confirmation of configuration data upload

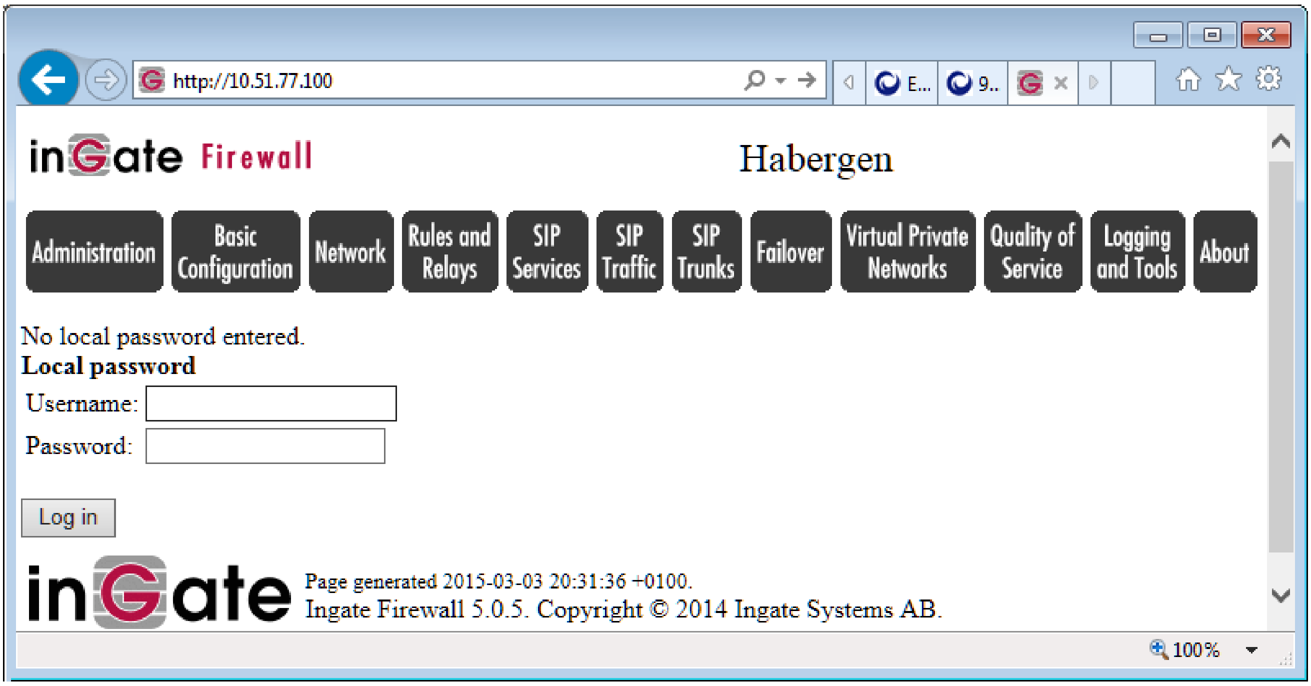
Click on **OK**. The default web browser will launch and navigate you to the SIParator’s web interface.

5.3 Ingate Administration Web Interface

5.3.1 Applying the Configuration

Although the configuration data has been uploaded to the SBC, it must still be explicitly applied before the SBC's behavior will change.

Log into the web interface with the administrative password that you selected earlier (in Figure 5).



Habergen

No local password entered.

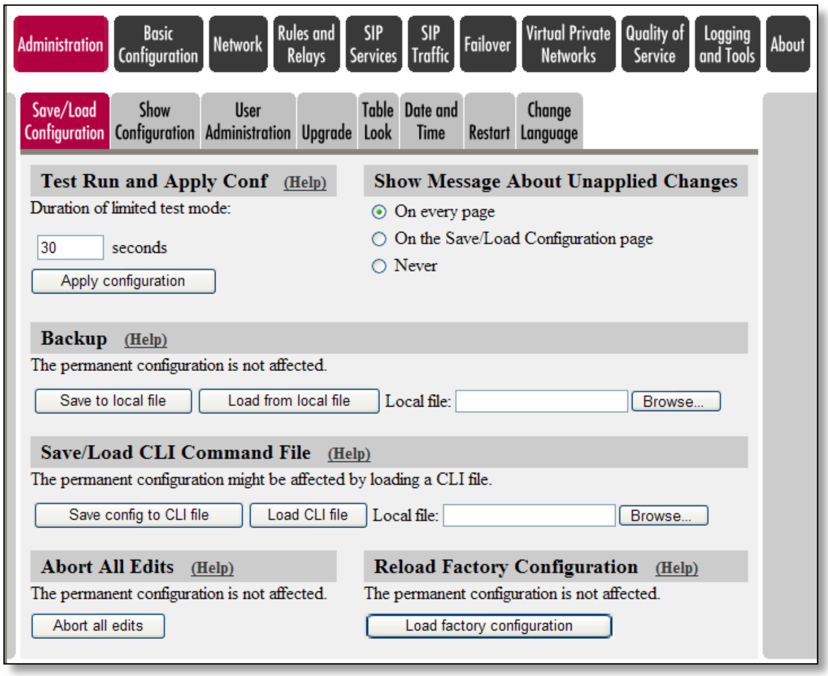
Local password

Username:

Password:

Page generated 2015-03-03 20:31:36 +0100.

Ingate Firewall 5.0.5. Copyright © 2014 Ingate Systems AB.



Test Run and Apply Conf (Help)

Duration of limited test mode:

30 seconds

Show Message About Unapplied Changes

● On every page

○ On the Save/Load Configuration page

○ Never

Backup (Help)

The permanent configuration is not affected.

Local file:

Save/Load CLI Command File (Help)

The permanent configuration might be affected by loading a CLI file.

Local file:

Abort All Edits (Help)

The permanent configuration is not affected.

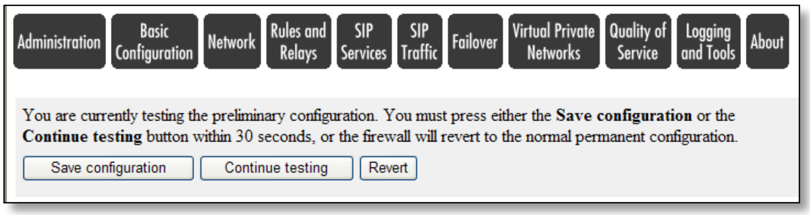
Reload Factory Configuration (Help)

The permanent configuration is not affected.

Figure 12. Applying the uploaded configuration

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

A window will appear (Figure 13) requesting further input.



You are currently testing the preliminary configuration. You must press either the **Save configuration** or the **Continue testing** button within 30 seconds, or the firewall will revert to the normal permanent configuration.

Figure 13. Saving the configuration

Click the button labeled **Save configuration**.

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

Further configuration settings must now be applied through the web interface.

6 Set SBC Options to work with Office 365 UM

6.1 Configuring SIP Signaling Encryption (TLS)

Transport Layer Security (TLS) must be used to secure the signaling between the SIParator and Office 365 Exchange UM.

To configure TLS between the Ingate SIParator and Office 365 Exchange UM, the following conditions must be met:

- A suitable **digital certificate** must be deployed on Ingate SIParator.
- Ingate SIParator must have the **SIP Trunking Module** deployed to provide routing rules, basic security policies, and other features.
- Ingate SIParator must have the **Enhanced SIP Security Module** deployed to provide TLS and SRTP encryption functionality.
- Ingate SIParator must be able to identify the Office 365 Exchange Online service by the service's fully qualified domain name (FQDN).

6.2 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. The list of supported CAs, and more information on the process, can be found at Get a Certificate for Exchange Online UM.

This certificate, and associated data (intermediate certificates) must be combined to form a Certificate Chain, and then must then be loaded into the SIParator.

Figure 14 represents the various steps in the process. These are described below the figure.

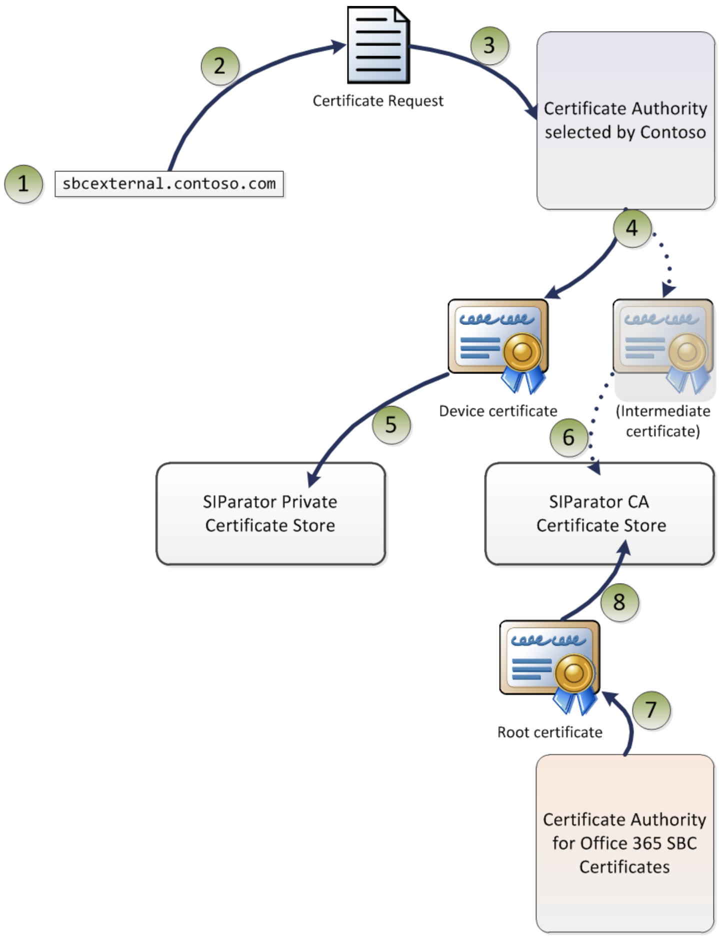

2
3
Certificate Request
Certificate Authority selected by Contoso
1
sbcexternal.contoso.com
4
Device certificate
(Intermediate certificate)
5
6
SIParator Private Certificate Store
SIParator CA Certificate Store
8
7
Root certificate
Certificate Authority for Office 365 SBC Certificates

Figure 14. Certificate management for SIParator connectivity to Office 365 UM

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 the CA. The CA will charge a fee to generate a certificate.

4. The CA will issue a signed certificate that contains the SBC's FQDN. In Figure 14, that is shown as the *Device certificate*. The CA will also issue at least one *Intermediate certificate* that links the device certificate to the CA's root certificate.

5. Combine the SBC *Device Certificate* with the *Intermediate Certificate* to create a Certificate Chain.

6. Load the device certificate into the SBC's Private Certificate Store.

7. Load the new *Intermediate Certificate Chain* into the SBC's CA Certificate Store.

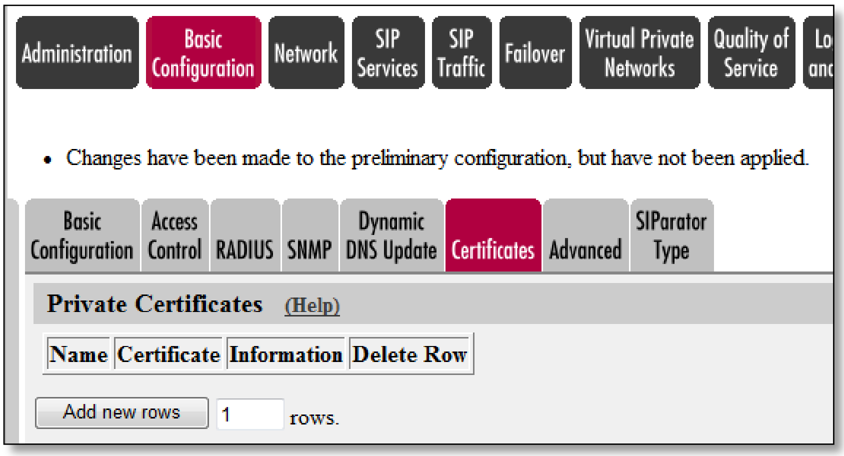
8. Download a *Root certificate*, from the CA used to sign the Office 365 certificates.

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

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

6.3 Creating a Certificate Request

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



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

Private Certificates (Help)

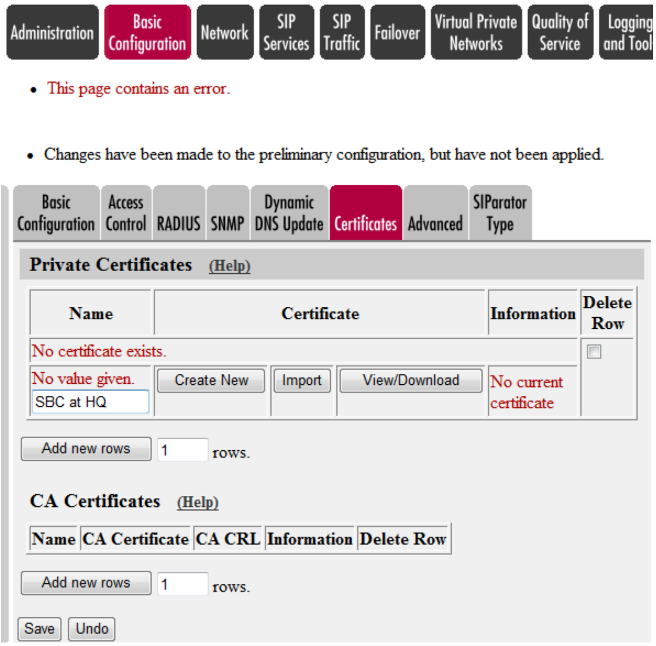
Name	Certificate	Information	Delete Row

1 rows.

Figure 15. 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 16), enter an identifying *Name* (e.g. **SBC at HQ**) for the new certificate and click **Create New**.



- This page contains an error.

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

Private Certificates (Help)

Name	Certificate			Information	Delete Row
No certificate exists.					☐
No value given. SBC at HQ	Create New	Import	View/Download	No current certificate	

1 rows.

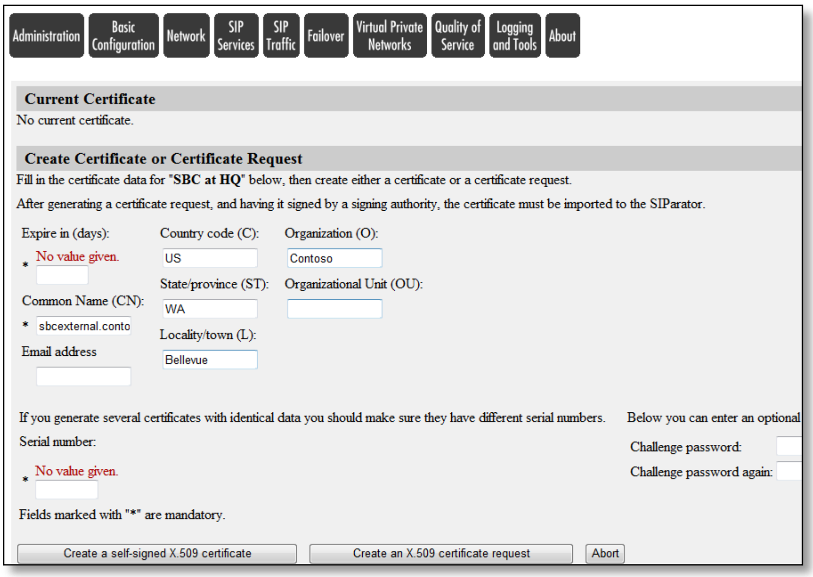
CA Certificates (Help)

Name	CA Certificate	CA CRL	Information	Delete Row

1 rows.

Figure 16. Adding a private certificate

Fill in the resulting *Create Certificate or Certificate Request* form (Figure 17) as described below.



Current Certificate

No current certificate.

Create Certificate or Certificate Request

Fill in the certificate data for "**SBC at HQ**" below, then create either a certificate or a certificate request.

After generating a certificate request, and having it signed by a signing authority, the certificate must be imported to the SIParator.

Expire in (days): * No value given.

Common Name (CN): * sbcexternal.conto

Email address

Country code (C): US

State/province (ST): WA

Locality/town (L): Bellevue

Organization (O): Contoso

Organizational Unit (OU):

If you generate several certificates with identical data you should make sure they have different serial numbers.

Serial number: * No value given.

Below you can enter an optional

Challenge password:

Challenge password again:

Fields marked with "*" are mandatory.

Create a self-signed X.509 certificate
Create an X.509 certificate request
Abort

Figure 17. 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 Office 365 Exchange UM, 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 in Figure 14.

There are also some optional fields, e.g.

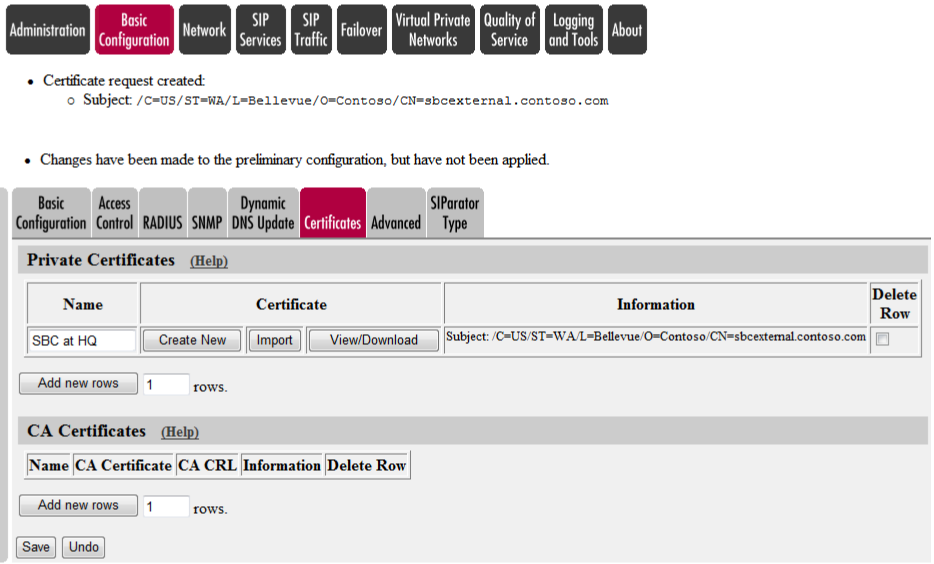
- The *Country Code (C)* field should contain the two-letter country code[3] for your organization's location (e.g. US for United States, GB for United Kingdom, JP for Japan, etc.).
- The *Organization (O)* field should contain the name of your organization.

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 in Figure 14.

After a short pause, details of the certificate request will be displayed (Figure 18).

[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] https://www.iso.org/obp/ui/



- Certificate request created:
  - Subject: /C=US/ST=WA/L=Bellevue/O=Contoso/CN=sbcexternal.contoso.com

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

Private Certificates (Help)

Name	Certificate	Information	Delete Row
SBC at HQ	Create New Import View/Download	Subject: /C=US/ST=WA/L=Bellevue/O=Contoso/CN=sbcexternal.contoso.com	☐

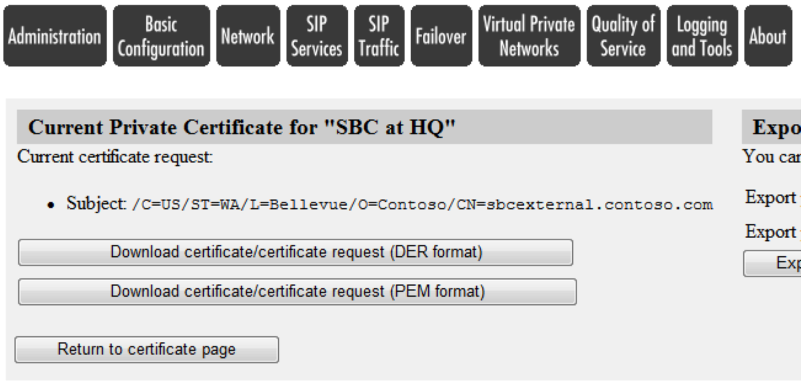
CA Certificates (Help)

Name	CA Certificate	CA CRL	Information	Delete Row

Figure 18. 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**.



Current Private Certificate for "SBC at HQ"

Current certificate request:

- Subject: /C=US/ST=WA/L=Bellevue/O=Contoso/CN=sbcexternal.contoso.com

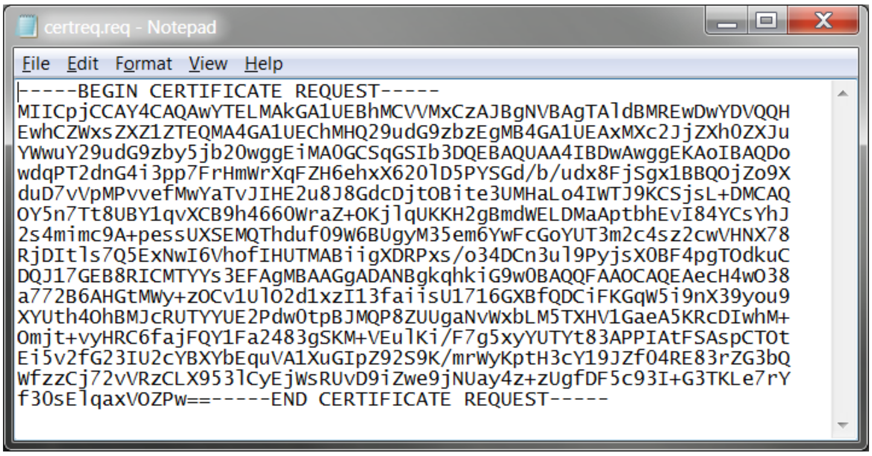
Download certificate/certificate request (DER format)
Download certificate/certificate request (PEM format)
Return to certificate page
Expo
You car
Export
Export
Exp

Figure 19. Viewing the certificate request

When the current certificate request is displayed (Figure 19), 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.req`. 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.



```
-----BEGIN CERTIFICATE REQUEST-----
MIICpjCCAY4CAQAwYTELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMREwDwYDVQQH
EwhCZWxsZXZ1ZTEQMA4GA1UEChMHQ29udG9zbzEgMB4GA1UEAxMXc2JjZXh0ZXJu
YWwuY29udG9zby5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDo
wdqPT2dnG4i3pp7FrHmWrXqFZH6ehxX620lD5PYSGd/b/udx8FjSgx1BBQ0jZo9X
duD7vVpMPvvefMwYaTvJIHE2u8J8GdcDjtOBite3UMHaLo4IWTJ9KCSjsL+DMCAQ
OY5n7Tt8UBY1qvXCB9h4660WraZ+OKjlqUKKH2gBmdWELDMaAptbhEvI84YCsYhJ
2s4mimc9A+pessUXSEMQThdufO9W6BUgyM35em6YwFcGoYUT3m2c4sz2cwVHNX78
RjDItls7Q5ExNwI6VhofIHUTMABiigXDRPxs/o34DCn3ul9PyjsX0BF4pgTOdkuC
DQJ17GEB8RICMTYYs3EFAgMBAAGgADANBgkqhkiG9w0BAQQFAAOCAQEAecH4wO38
a772B6AHGtMWy+zOCv1UlO2d1xzI13faiisU1716GXBfQDCiFKGqW5i9nX39you9
XYUth4OhBMJcRUTYYUE2Pdw0tpBJMQP8ZUUgaNvWxbLM5TXHV1GaeA5KRcDIwhM+
Omjt+vyHRC6fajFQY1Fa2483gSKM+VEulKi/F7g5xyYUTYt83APPIAtFSAspCTOt
Ei5v2fG23IU2cYBXYbEquVA1XuGIpZ92S9K/mrWyKptH3cY19JZf04RE83rZG3bQ
WfzzCj72vVRzCLX953lCyEjWsRUvD9iZwe9jNUay4z+zUgfDF5c93I+G3TKLe7rY
f30sElqaxVOZPw==-----END CERTIFICATE REQUEST-----
```

Figure 20. 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 with Office 365. This corresponds to step 3 in Figure 14.

The process of generating and downloading a certificate varies from one CA to another: please consult the chosen CA's web site for details.

6.4 Creating an Intermediate Certificate Chain

The Ingate SIParator has the ability to independently import the Intermediate Certificate and attach them to the SBC Device Certificate and building up the certificate chain. A t **Basic Configuration > Certificates**, under the column "Certificate", there is a button "Import".

Overall;

It is not good idea to include the root cert in the combined file. However, if done by accident, it can be removed in a text editor. Open `SBC_Device_and_Interm_combined.crt` in the text editor and remove the last occurrence of `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` and the base64 encoded text block in between.

6.5 Importing SBC Device CA-Signed Certificate

Download the certificate from the CA, saving it locally as a file or several files. This corresponds to step 4 in Figure 14.

The certificate consists of the *Device certificate* and also at least one *Intermediate certificate* that links the device certificate to the CA's root certificate. There might be several *Intermediate certificates.* The different certificates can be bundled into one or more files. Figure **21** illustrates three examples how the certificates can be bundled. Each files must be imported separately. First the *Device certificate* must be imported and after that the *Intermediate certificates* depending how they are located in the files.

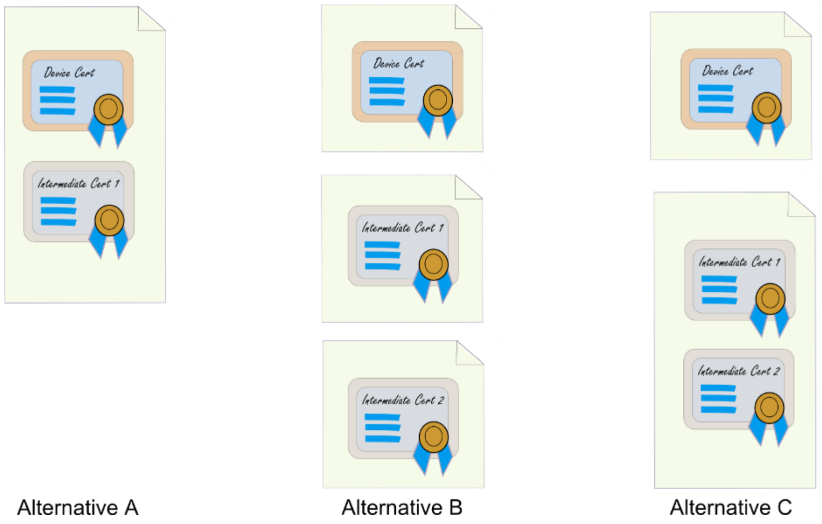


Figure 21. Different alternatives how certificates can be bundled

You must first import the *Device certificate.* If any *Intermediate certificates* is bundled into same file it will also be imported at same time.

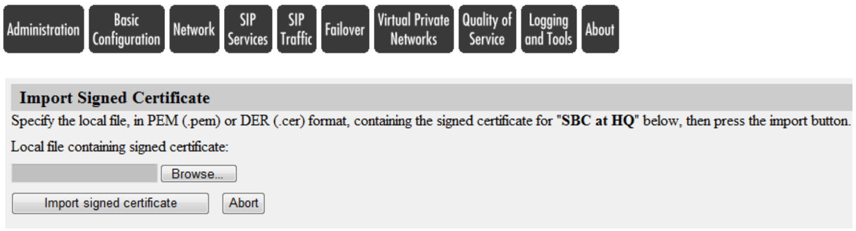
Place the file (files) on the computer running the web browser that is being used to configure the SIParator (or in a place that is accessible to it).

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 22), click on the **Browse…** button and navigate to the one of the files that you downloaded, the one that includes the *Device certificate*.



Import Signed Certificate

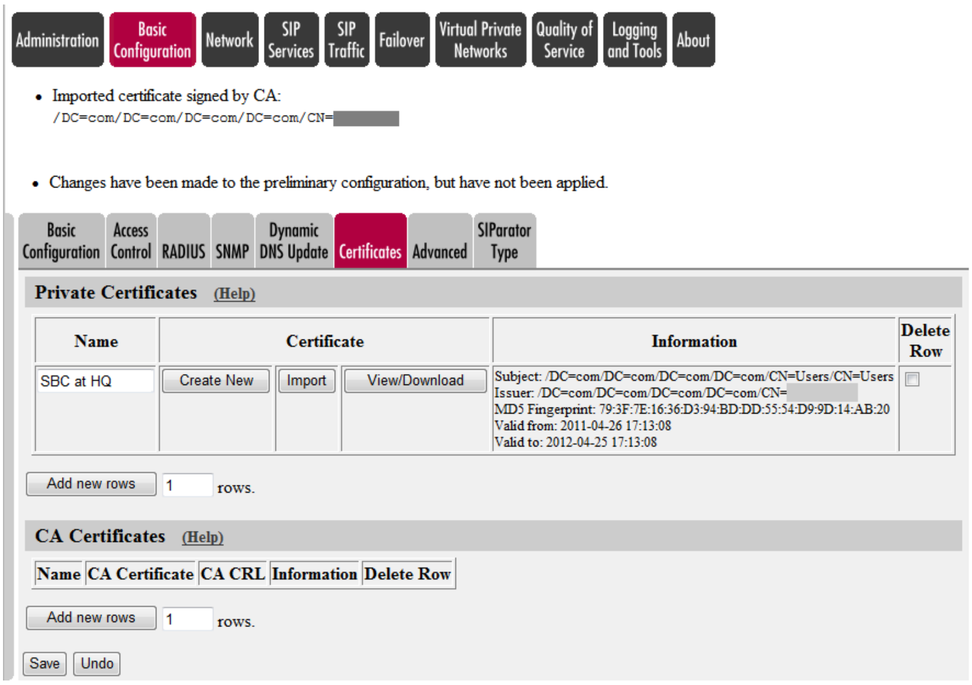
Specify the local file, in PEM (.pem) or DER (.cer) format, containing the signed certificate for "**SBC at HQ**" below, then press the import button.

Local file containing signed certificate:

Figure 22. 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 in Figure 14.

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



- Imported certificate signed by CA:
  `/DC=com/DC=com/DC=com/DC=com/CN=`[redacted]

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

Private Certificates (Help)

Name	Certificate			Information	Delete Row
SBC at HQ	Create New	Import	View/Download	Subject: /DC=com/DC=com/DC=com/DC=com/CN=Users/CN=Users Issuer: /DC=com/DC=com/DC=com/DC=com/CN=[redacted] MD5 Fingerprint: 79:3F:7E:16:36:D3:94:BD:DD:55:54:D9:9D:14:AB:20 Valid from: 2011-04-26 17:13:08 Valid to: 2012-04-25 17:13:08	□

Add new rows 1 rows.

CA Certificates (Help)

Name	CA Certificate	CA CRL	Information	Delete Row

Add new rows 1 rows.

Figure 23. Certificate after import into the SIParator

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

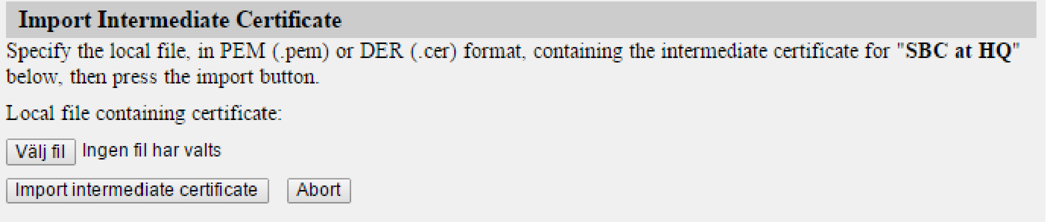
6.6 *Importing Intermediate Certificates*

You must now import the intermediate certificates into the Private Certificate store if not all of them was bundled into same file as the Device Ceritficate, as in Alternative A in Figure **21**.

For each intermediate certificate (that is for each file):

Under **Basic Configuration** > **Certificates** in the Ingate control panel, under *Private Certificates*, go to the Row with the SBC Device Certificate Request and under the Certificate column click **Import** to add the Intermediate Certificate.

On the screen that is displayed under **Import Intermediate Certificate**, click the **Browse…** button and then navigate to the file for *Intermediate certificate*, and select it.



Import Intermediate Certificate

Specify the local file, in PEM (.pem) or DER (.cer) format, containing the intermediate certificate for "**SBC at HQ**" below, then press the import button.

Local file containing certificate:

Figure 24. Preparing to import the Intemediate certificate

When the file name is displayed under *Local file containing certificate*, click on the button labeled **Import intermediate certificate**. This corresponds to step 6 in Figure 14.

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

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

6.7 Importing a Root Certificate

Communication between the SBC and Office 365 Exchange UM will require mutual TLS. Not only will Office 365 authenticate the SBC (by means of the device certificate that you imported), but your SBC must also authenticate Office 365. 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 Office 365.

There are some options:

1) Baltimore CyberTrust Root CA

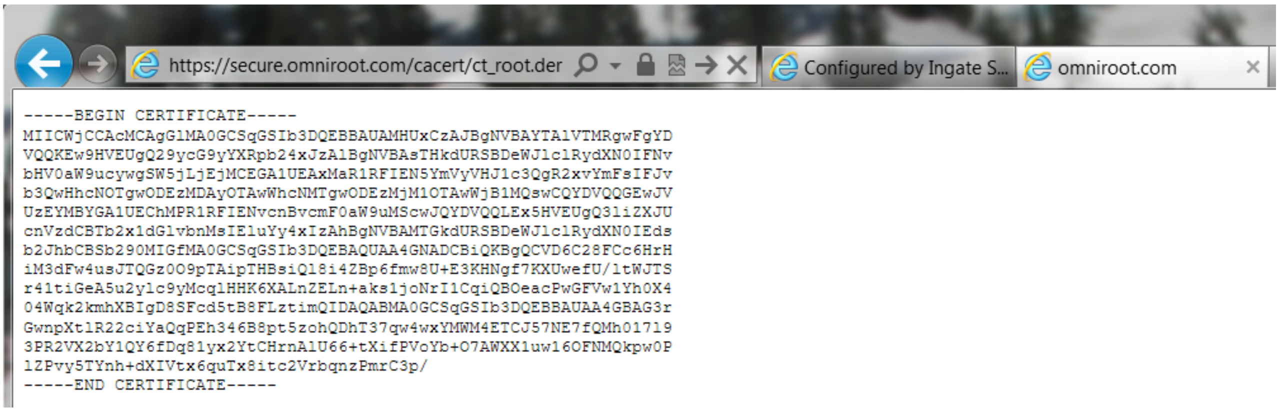
To obtain this certificate, use a web browser to navigate to

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

2) GTE CyberTrust Root CA

To obtain this certificate, use a web browser to navigate (Figure 25) to https://secure.omniroot.com/cacert/ct_root.der.

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


https://secure.omniroot.com/cacert/ct_root.der
Configured by Ingate S...
omniroot.com

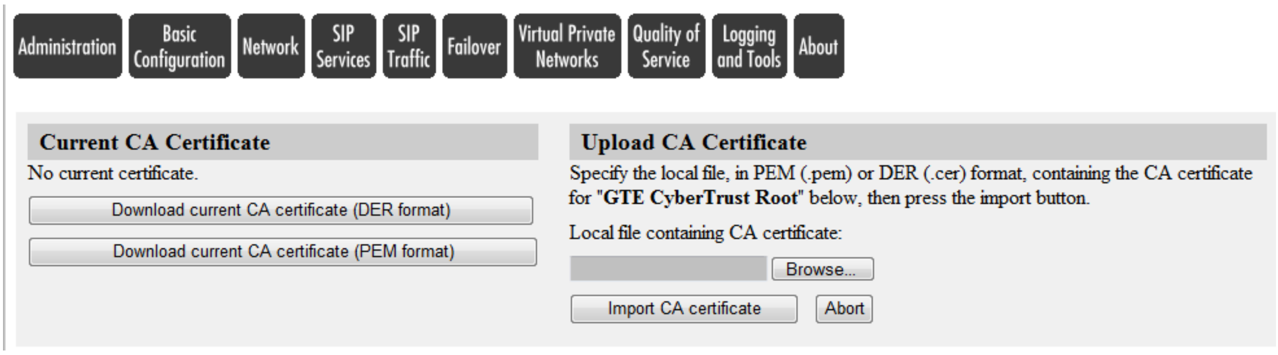
```
-----BEGIN CERTIFICATE-----
MIICWjCCAcMCAgGlMA0GCSqGSIb3DQEBBAUAMHUxCzAJBgNVBAYTAlVTMRgwFgYD
VQQKEw9HVEUgQ29ycG9yYXRpb24xJzAlBgNVBAsTHkdURSBDeWJlclRydXN0IFNv
bHV0aW9ucywgSW5jLjEjMCEGA1UEAxMaR1RFIEN5YmVyVHJ1c3QgR2xvYmFsIFJv
b3QwHhcNOTgwODEzMDAyOTAwWhcNMTgwODEzMjM1OTAwWjB1MQswCQYDVQQGEwJV
UzEYMBYGA1UEChMPR1RFIENvcnBvcmF0aW9uMScwJQYDVQQLEx5HVEUgQ3liZXJU
cnVzdCBTb2x1dGlvbnMsIEluYy4xIzAhBgNVBAMTGkdURSBDeWJlclRydXN0IEds
b2JhbCBSb290MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCVD6C28FCc6HrH
iM3dFw4usJTQGz0O9pTAipTHBsiQl8i4ZBp6fmw8U+E3KHNgf7KXUwefU/ltWJTS
r41tiGeA5u2ylc9yMcqlHHK6XALnZELn+aks1joNrI1CqiQBOeacPwGFVw1Yh0X4
04Wqk2kmhXBIgD8SFcd5tB8FLztimQIDAQABMA0GCSqGSIb3DQEBBAUAA4GBAG3r
GwnpXtlR22ciYaQqPEh346B8pt5zohQDhT37qw4wxYMWM4ETCJ57NE7fQMh017l9
3PR2VX2bY1QY6fDq81yx2YtCHrnAlU66+tXifPVoYb+O7AWXX1uw16OFNMQkpw0P
lZPvy5TYnh+dXIVtx6quTx8itc2VrbqnzPmrC3p/
-----END CERTIFICATE-----
```

Figure 25. 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.der`. This corresponds to step 7 in Figure 14.

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. **GTE CyberTrust Root**). Then, click the button (under the *CA Certificate* column) labeled **Change/View**.



Current CA Certificate

No current certificate.

Download current CA certificate (DER format)

Download current CA certificate (PEM format)

Upload CA Certificate

Specify the local file, in PEM (.pem) or DER (.cer) format, containing the CA certificate for "**GTE CyberTrust Root**" below, then press the import button.

Local file containing CA certificate:

Browse...

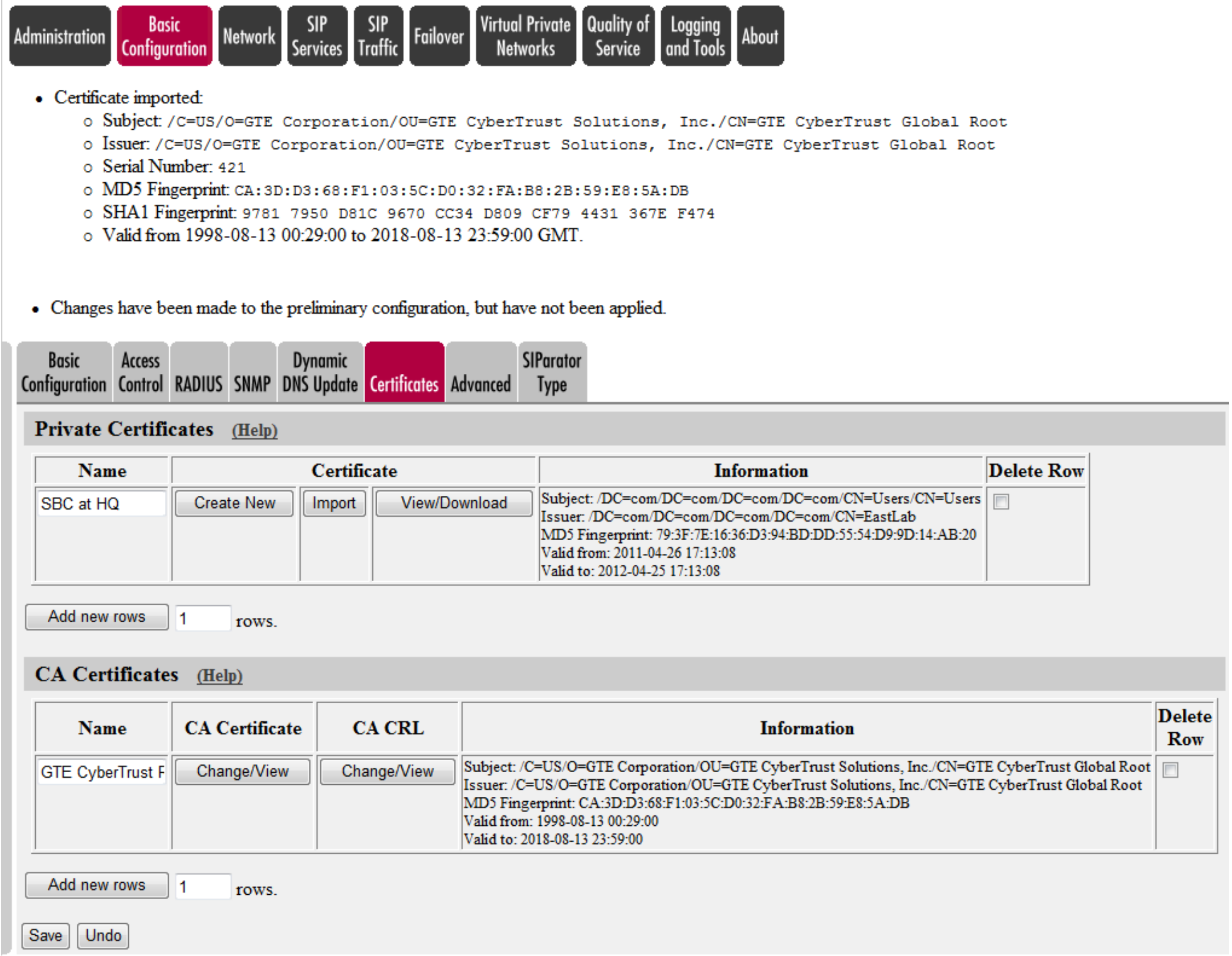
Import CA certificate | Abort

Figure 26. Preparing to import the root certificate

On the screen that is displayed (Figure 26), click the **Browse…** button and then navigate to the `ct_root.der` 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 in Figure 14.

After a pause, details of the newly-imported root certificate should be shown, along with those of your CA-signed device certificate (Figure 27).



- Certificate imported:
  - Subject: `/C=US/O=GTE Corporation/OU=GTE CyberTrust Solutions, Inc./CN=GTE CyberTrust Global Root`
  - Issuer: `/C=US/O=GTE Corporation/OU=GTE CyberTrust Solutions, Inc./CN=GTE CyberTrust Global Root`
  - Serial Number: `421`
  - MD5 Fingerprint: `CA:3D:D3:68:F1:03:5C:D0:32:FA:B8:2B:59:E8:5A:DB`
  - SHA1 Fingerprint: `9781 7950 D81C 9670 CC34 D809 CF79 4431 367E F474`
  - Valid from 1998-08-13 00:29:00 to 2018-08-13 23:59:00 GMT.

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

Private Certificates (Help)

Name	Certificate			Information	Delete Row
SBC at HQ	Create New	Import	View/Download	Subject: /DC=com/DC=com/DC=com/DC=com/CN=Users/CN=Users Issuer: /DC=com/DC=com/DC=com/DC=com/CN=EastLab MD5 Fingerprint: 79:3F:7E:16:36:D3:94:BD:DD:55:54:D9:9D:14:AB:20 Valid from: 2011-04-26 17:13:08 Valid to: 2012-04-25 17:13:08	□

Add new rows 1 rows.

CA Certificates (Help)

Name	CA Certificate	CA CRL	Information	Delete Row
GTE CyberTrust F	Change/View	Change/View	Subject: /C=US/O=GTE Corporation/OU=GTE CyberTrust Solutions, Inc./CN=GTE CyberTrust Global Root Issuer: /C=US/O=GTE Corporation/OU=GTE CyberTrust Solutions, Inc./CN=GTE CyberTrust Global Root MD5 Fingerprint: CA:3D:D3:68:F1:03:5C:D0:32:FA:B8:2B:59:E8:5A:DB Valid from: 1998-08-13 00:29:00 Valid to: 2018-08-13 23:59:00	□

Add new rows 1 rows.

Save | Undo

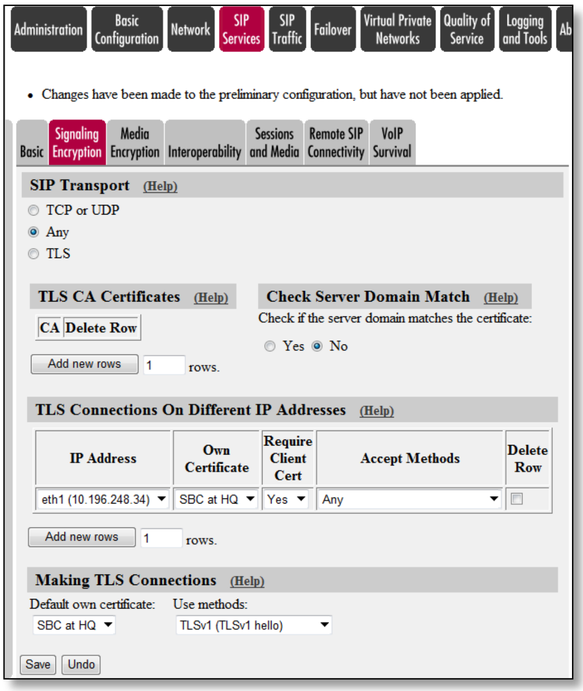
Figure 27. After importing the root certificate

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).

6.8 TLS Setup

Navigate to **SIP Services** > **Signaling Encryption** (Figure 28).



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

SIP Transport (Help)

○ TCP or UDP
● Any
○ TLS

TLS CA Certificates (Help)

CA	Delete Row

Add new rows 1 rows.

Check Server Domain Match (Help)

Check if the server domain matches the certificate:

○ Yes ● No

TLS Connections On Different IP Addresses (Help)

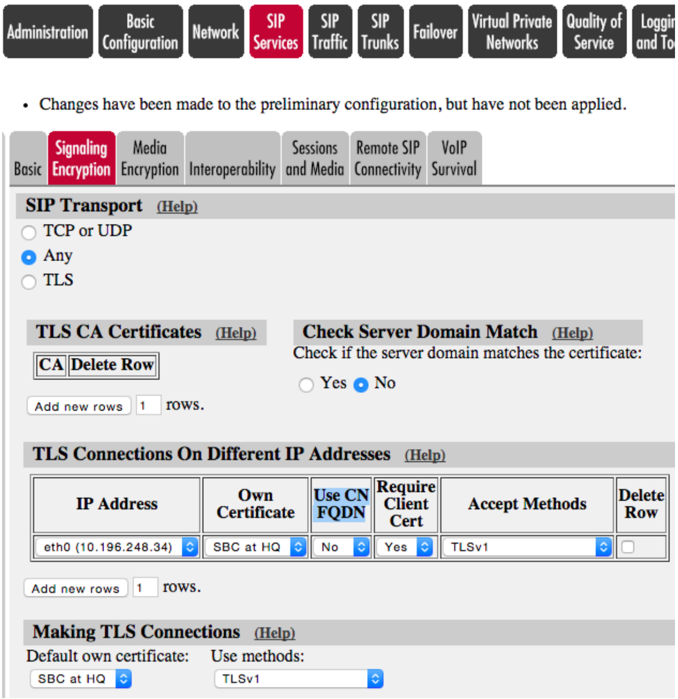
IP Address	Own Certificate	Require Client Cert	Accept Methods	Delete Row
eth1 (10.196.248.34)	SBC at HQ	Yes	Any	□

Add new rows 1 rows.

Making TLS Connections (Help)

Default own certificate: SBC at HQ
Use methods: TLSv1 (TLSv1 hello)

Save Undo



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

SIP Transport (Help)

○ TCP or UDP
● Any
○ TLS

TLS CA Certificates (Help)

CA	Delete Row

Add new rows 1 rows.

Check Server Domain Match (Help)

Check if the server domain matches the certificate:

○ Yes ● No

TLS Connections On Different IP Addresses (Help)

IP Address	Own Certificate	Use CN FQDN	Require Client Cert	Accept Methods	Delete Row
eth0 (10.196.248.34)	SBC at HQ	No	Yes	TLSv1	□

Add new rows 1 rows.

Making TLS Connections (Help)

Default own certificate: SBC at HQ
Use methods: TLSv1

Ingate firmware <= version 4.10.2 Ingate firmware >= version 5.0.1

Figure 28. Configuring signaling encryption

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

Under *TLS CA Certificates*, select the root certificate that you imported earlier (see chapter 6.7 Importing a Root Certificate).

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

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

Set *IP Address* to that of the external interface (see Figure 7).

Set *Own Certificate* to be the device certificate that you imported earlier (*The process of generating* and downloading a certificate varies from one CA to another: please consult the chosen CA's web site for details.)

Set *Use CN FQDN* to **No**. (Ingate firmware >= v5.0.1)

Set *Require Client Cert* to be **Yes**.

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 **TLSv1 (TLSv1 hello)**. (Ingate firmware <= version 4.10.2)

Set Use methods to be **TLSv1**. (Ingate firmware >= version 5.0.1)

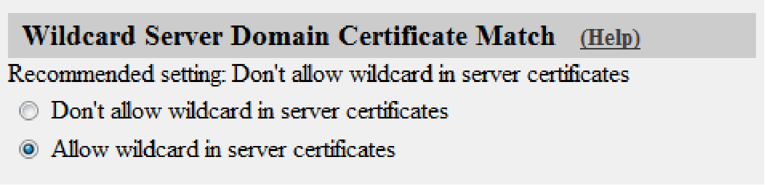
Click **Save**.

The *Check Server Domain Match* setting (**Yes**) that you configured above will force the SIParator only to accept certificates from Office 365 if the name in the certificate matches the domain from which the certificate was communicated. This provides additional security. The name in the certificates used by Office 365 for Exchange UM is `*.um.outlook.com`, which contains the "wildcard" character `*`. By default, SIParator does not process wildcards in domain matching, so you will also need to enable this capability.

Note that because SSLv3 and prior are considered unsafe, and in light of the POODLE CVS, Encryption methods should use TLSv1 only.

Navigate to **Configuration** > **SIP Services** > **Interoperability**.

Under *Wildcard Server Domain Certificate Match*[5], select **Allow wildcard in server certificates**.



Wildcard Server Domain Certificate Match (Help)

Recommended setting: Don't allow wildcard in server certificates

○ Don't allow wildcard in server certificates

● Allow wildcard in server certificates

Figure 29. Enabling wildcards in domain certificate matching

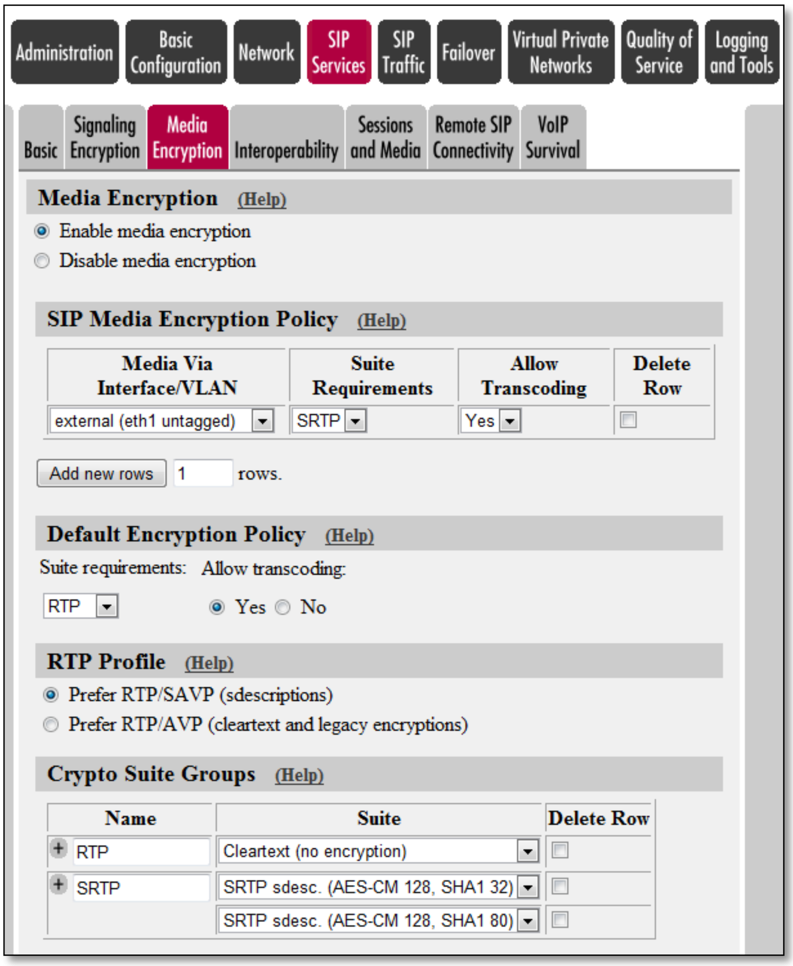
Click **Save**.

6.9 Configuring Media Encryption (SRTP)

Secure Real Time Protocol (SRTP) must be used to secure media (audio data) between the SIParator and Office 365 Exchange UM. 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[6].

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

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



Media Encryption (Help)

● Enable media encryption

○ Disable media encryption

SIP Media Encryption Policy (Help)

Media Via Interface/VLAN	Suite Requirements	Allow Transcoding	Delete Row
external (eth1 untagged)	SRTP	Yes	□

Add new rows 1 rows.

Default Encryption Policy (Help)

Suite requirements: RTP

Allow transcoding: ● Yes ○ No

RTP Profile (Help)

● Prefer RTP/SAVP (sdescriptions)

○ Prefer RTP/AVP (cleartext and legacy encryptions)

Crypto Suite Groups (Help)

Name	Suite	Delete Row
+ RTP	Cleartext (no encryption)	□
+ SRTP	SRTP sdesc. (AES-CM 128, SHA1 32)	□
	SRTP sdesc. (AES-CM 128, SHA1 80)	□

Figure 30. Configuring media encryption

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

Under *Crypto Suite Groups*, configure as follows:

Create a group for RTP, if necessary[7]

Under *Name*, enter **RTP**

Under *Suite*, select **Cleartext (no encryption)**

Click **Add New Row**, if necessary

Create a group for SRTP

Under *Name*, enter **SRTP**

Under *Suite*, select **SRTP sdec (AES-CM 128, SHA1 32)**

Click the **+** beside the *SRTP* name to add an additional entry

Under *Suite*, select **SRTP sdec (AES-CM 128, SHA1 80)**

[7] The factory default setup should include a cleartext group that you can use.

Click **Save**

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

Under *Media Via Interface/VLAN*, select the external interface (Eth1)

Under *Suite Requirements*, select **SRTP**

Under *Default Encryption Policy*, configure as follows:

Under *Suite Requirements*, select **RTP**

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

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

Click **Save.**

6.10 Configuring Local REFER Handling

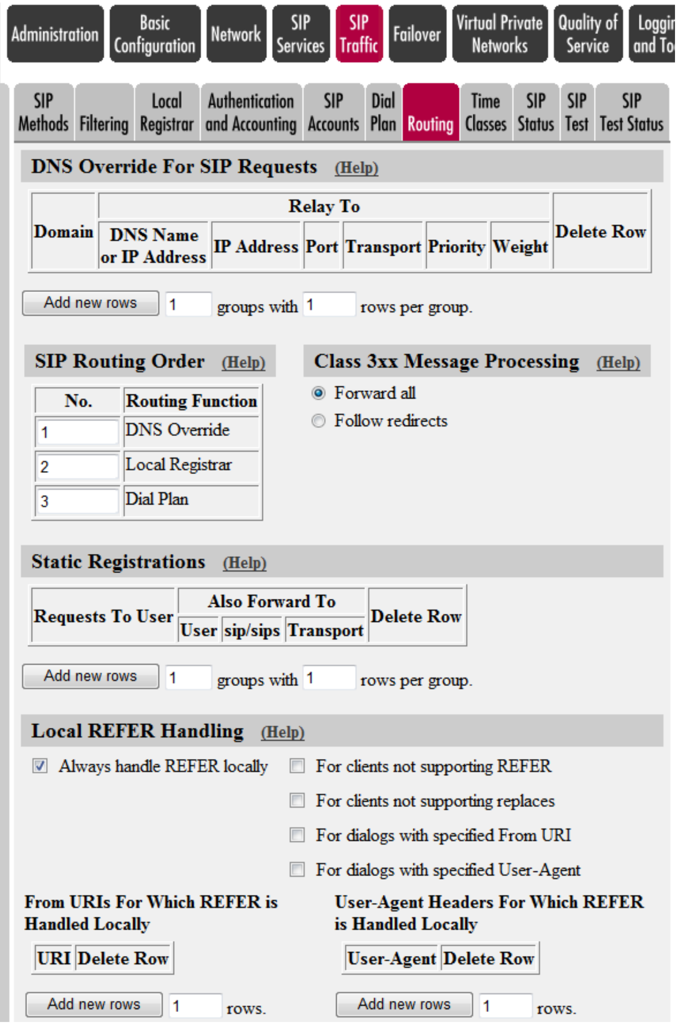
There are several scenarios in which Office 365 Exchange UM needs to transfer a call in progress. UM does this by sending a SIP REFER **message**. Often, the target of the transfer is on the PBX, or reachable through the PBX's connection to the telephone network. But sometimes, the target of the transfer is a SIP address "outside" the SBC. For example, you might configure a hosted fax service for UM-enabled users[8].

The simplest way to accommodate both internal and external SIP transfers is to configure the SIParator to handle processing of the REFER, rather than passing it through to the VoIP gateway or IP PBX. By acting on (some of) the SIP messages sent from UM, rather than passing them to the VoIP gateway or IP PBX, the SIParator acts as a "back-to-back user agent" (B2BUA).

To configure this behavior, navigate to **Configuration** > **SIP Traffic** > **Routing**. (Figure 31).

Under *Local REFER Handling*, ensure that the **Always handle REFER locally** box is checked.

[8] See http://technet.microsoft.com/en-us/library/bb232022.aspx for further details.



DNS Override For SIP Requests (Help)

Domain	Relay To						Delete Row
	DNS Name or IP Address	IP Address	Port	Transport	Priority	Weight	

Add new rows 1 groups with 1 rows per group.

SIP Routing Order (Help)

No.	Routing Function
1	DNS Override
2	Local Registrar
3	Dial Plan

Class 3xx Message Processing (Help)

● Forward all

○ Follow redirects

Static Registrations (Help)

Requests To User	Also Forward To			Delete Row
	User	sip/sips	Transport	

Add new rows 1 groups with 1 rows per group.

Local REFER Handling (Help)

☑ Always handle REFER locally

□ For clients not supporting REFER

□ For clients not supporting replaces

□ For dialogs with specified From URI

□ For dialogs with specified User-Agent

From URIs For Which REFER is Handled Locally

URI	Delete Row

Add new rows 1 rows.

User-Agent Headers For Which REFER is Handled Locally

User-Agent	Delete Row

Add new rows 1 rows.

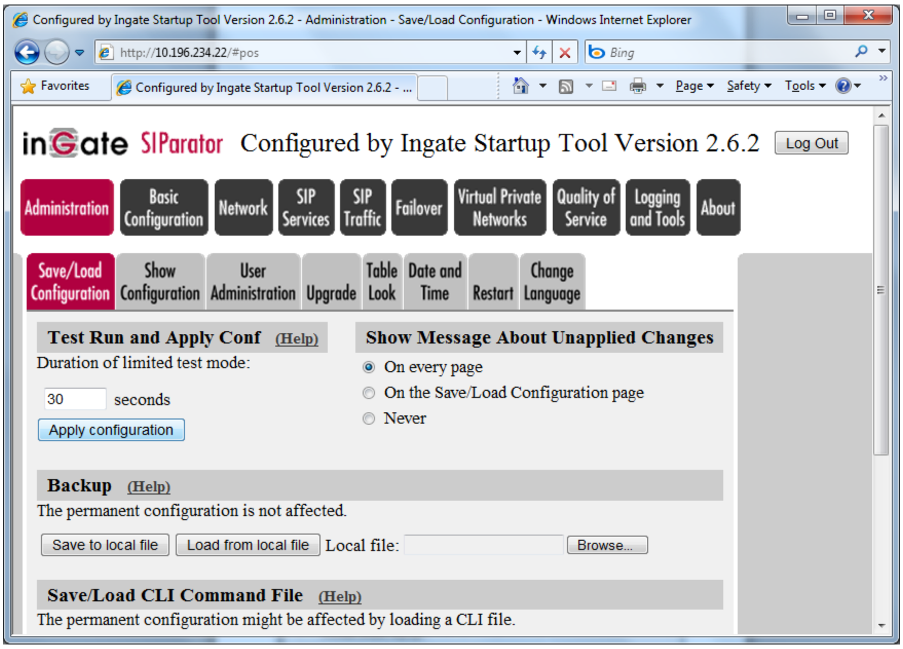
Figure 31. Configuring local REFER handling

If necessary (if the box was previously unchecked), click on **Save** (at the bottom of the page).

Your device is now ready for use with Office 365 Exchange UM.

6.11 Apply and save configuration

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



Test Run and Apply Conf (Help)

Duration of limited test mode:

30 seconds

Apply configuration

Show Message About Unapplied Changes

● On every page
○ On the Save/Load Configuration page
○ Never

Backup (Help)

The permanent configuration is not affected.

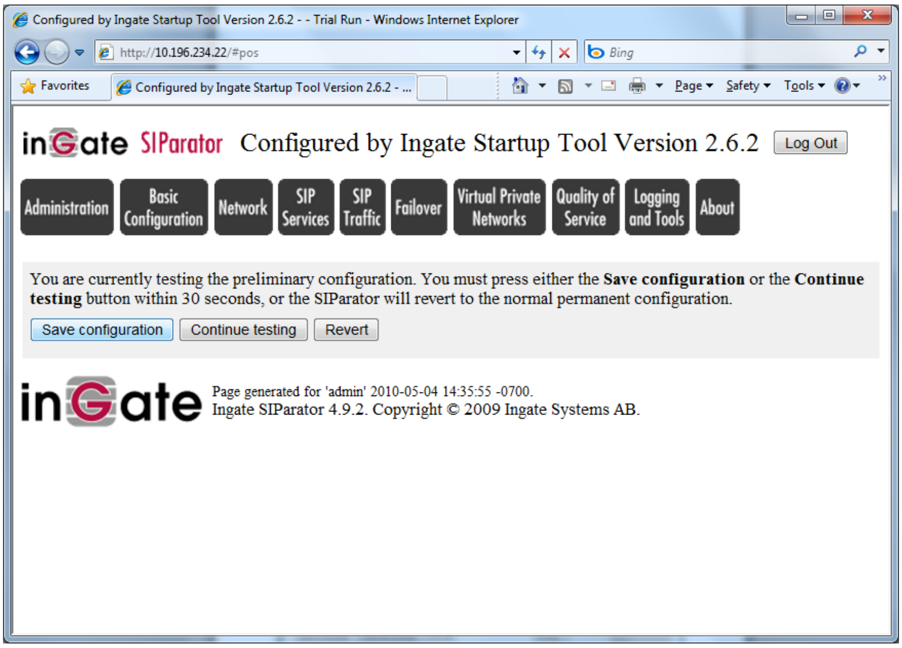
Save to local file | Load from local file | Local file: | Browse...

Save/Load CLI Command File (Help)

The permanent configuration might be affected by loading a CLI file.

Figure 32. Applying the configuration

When the configuration has been applied (Figure 33), click **Save configuration**.


Configured by Ingate Startup Tool Version 2.6.2 - - Trial Run - Windows Internet Explorer
http://10.196.234.22/#pos
Favorites
Configured by Ingate Startup Tool Version 2.6.2 - ...
inGate SIParator Configured by Ingate Startup Tool Version 2.6.2
Log Out
Administration
Basic Configuration
Network
SIP Services
SIP Traffic
Failover
Virtual Private Networks
Quality of Service
Logging and Tools
About

You are currently testing the preliminary configuration. You must press either the **Save configuration** or the **Continue testing** button within 30 seconds, or the SIParator will revert to the normal permanent configuration.

Save configuration | Continue testing | Revert

Page generated for 'admin' 2010-05-04 14:35:55 -0700.
Ingate SIParator 4.9.2. Copyright © 2009 Ingate Systems AB.

Figure 33. Saving the configuration

The SIParator should report: *Configuration applied and saved*.

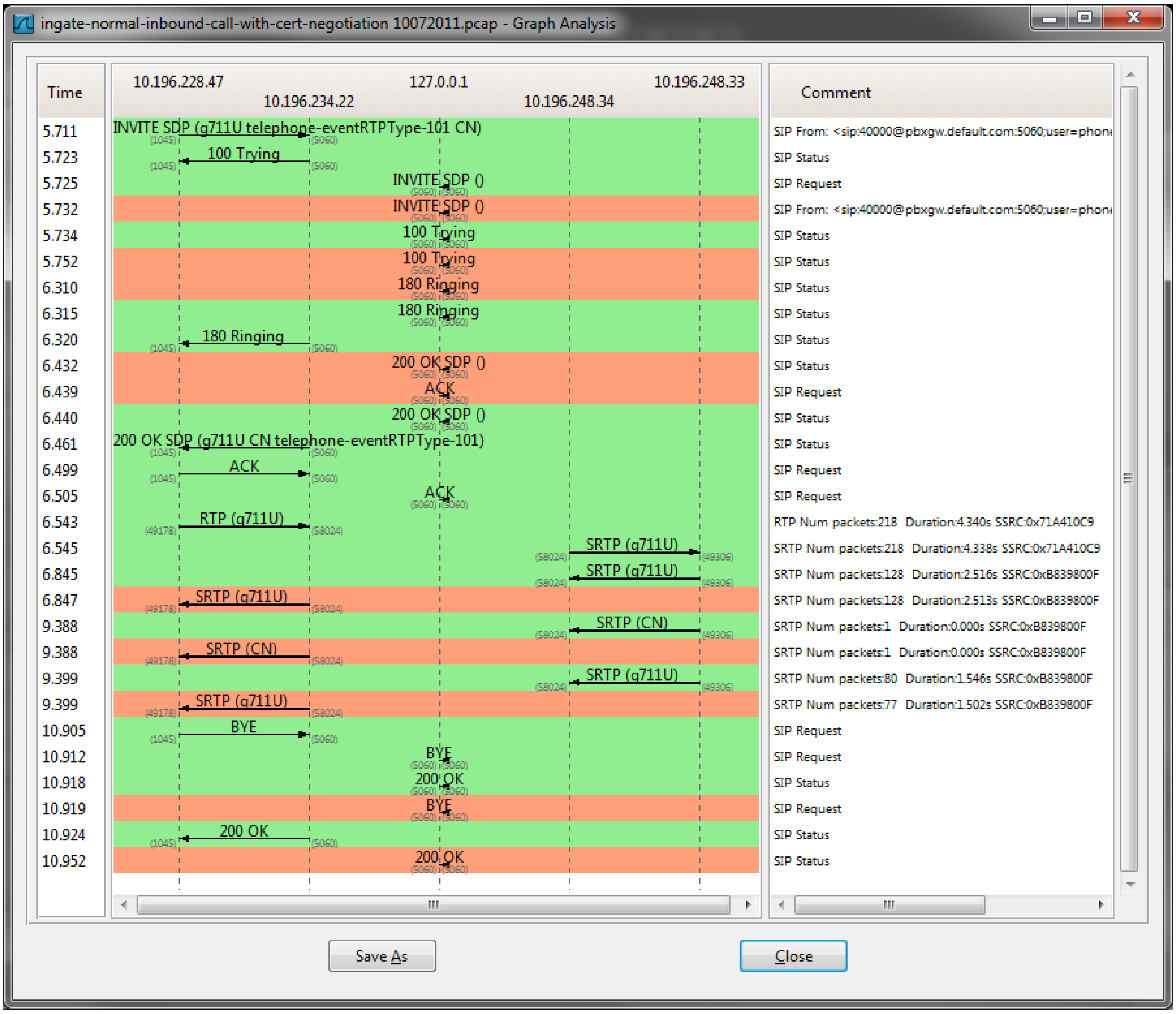
7 Verify SBC Configuration

7.1 Appendix. Call Flows for Troubleshooting

7.1.1 Make a Call

In the following packet capture example, obtained in a network topology used for testing, here are the systems and interfaces involved:

- Dialogic Gateway: **10.196.228.47**
- Ingate SIParator:
  - Internal (LAN) side: **10.196.234.22**
  - External (WAN) side: **10.196.248.34** (Internal IP for Testing)
- Office 365 UM SBC: **10.196.234.33** (Internal IP for Testing)
- Office 365 UM: Not seen – behind its own SBC.



ingate-normal-inbound-call-with-cert-negotiation 10072011.pcap - Graph Analysis
10.196.228.47
10.196.234.22
127.0.0.1
10.196.248.34
10.196.248.33
Save As
Close

Time		Comment
5.711	INVITE SDP (g711U telephone-eventRTPType-101 CN) (1045) (5060)	SIP From: <sip:40000@pbxgw.default.com:5060;user=phon
5.723	100 Trying (1045) (5060)	SIP Status
5.725	INVITE SDP () (5060) (5060)	SIP Request
5.732	INVITE SDP () (5060) (5060)	SIP From: <sip:40000@pbxgw.default.com:5060;user=phon
5.734	100 Trying (5060) (5060)	SIP Status
5.752	100 Trying (5060) (5060)	SIP Status
6.310	180 Ringing (5060) (5060)	SIP Status
6.315	180 Ringing (5060) (5060)	SIP Status
6.320	180 Ringing (1045) (5060)	SIP Status
6.432	200 OK SDP () (5060) (5060)	SIP Status
6.439	ACK (5060) (5060)	SIP Request
6.440	200 OK SDP () (5060) (5060)	SIP Status
6.461	200 OK SDP (g711U CN telephone-eventRTPType-101) (1045) (5060)	SIP Status
6.499	ACK (1045) (5060)	SIP Request
6.505	ACK (5060) (5060)	SIP Request
6.543	RTP (g711U) (49178) (58024)	RTP Num packets:218 Duration:4.340s SSRC:0x71A410C9
6.545	SRTP (g711U) (58024) (49306)	SRTP Num packets:218 Duration:4.338s SSRC:0x71A410C9
6.845	SRTP (g711U) (58024) (49306)	SRTP Num packets:128 Duration:2.516s SSRC:0xB839800F
6.847	SRTP (g711U) (49178) (58024)	SRTP Num packets:128 Duration:2.513s SSRC:0xB839800F
9.388	SRTP (CN) (58024) (49306)	SRTP Num packets:1 Duration:0.000s SSRC:0xB839800F
9.388	SRTP (CN) (49178) (58024)	SRTP Num packets:1 Duration:0.000s SSRC:0xB839800F
9.399	SRTP (g711U) (58024) (49306)	SRTP Num packets:80 Duration:1.546s SSRC:0xB839800F
9.399	SRTP (g711U) (49178) (58024)	SRTP Num packets:77 Duration:1.502s SSRC:0xB839800F
10.905	BYE (1045) (5060)	SIP Request
10.912	BYE (5060) (5060)	SIP Request
10.918	200 OK (5060) (5060)	SIP Status
10.919	BYE (5060) (5060)	SIP Request
10.924	200 OK (1045) (5060)	SIP Status
10.952	200 OK (5060) (5060)	SIP Status

7.1.2 Gateway and Ingate

1) Notice the SIP call flow between the Dialogic and the Ingate devices. Here the Dialogic DMG1000 calls the Ingate and eventually the call is answered. The SIP Protocol is over UDP and is not encrypted.
2) The Dialogic streams RTP to the Ingate ports, and the Ingate streams RTP to the Dialogic.

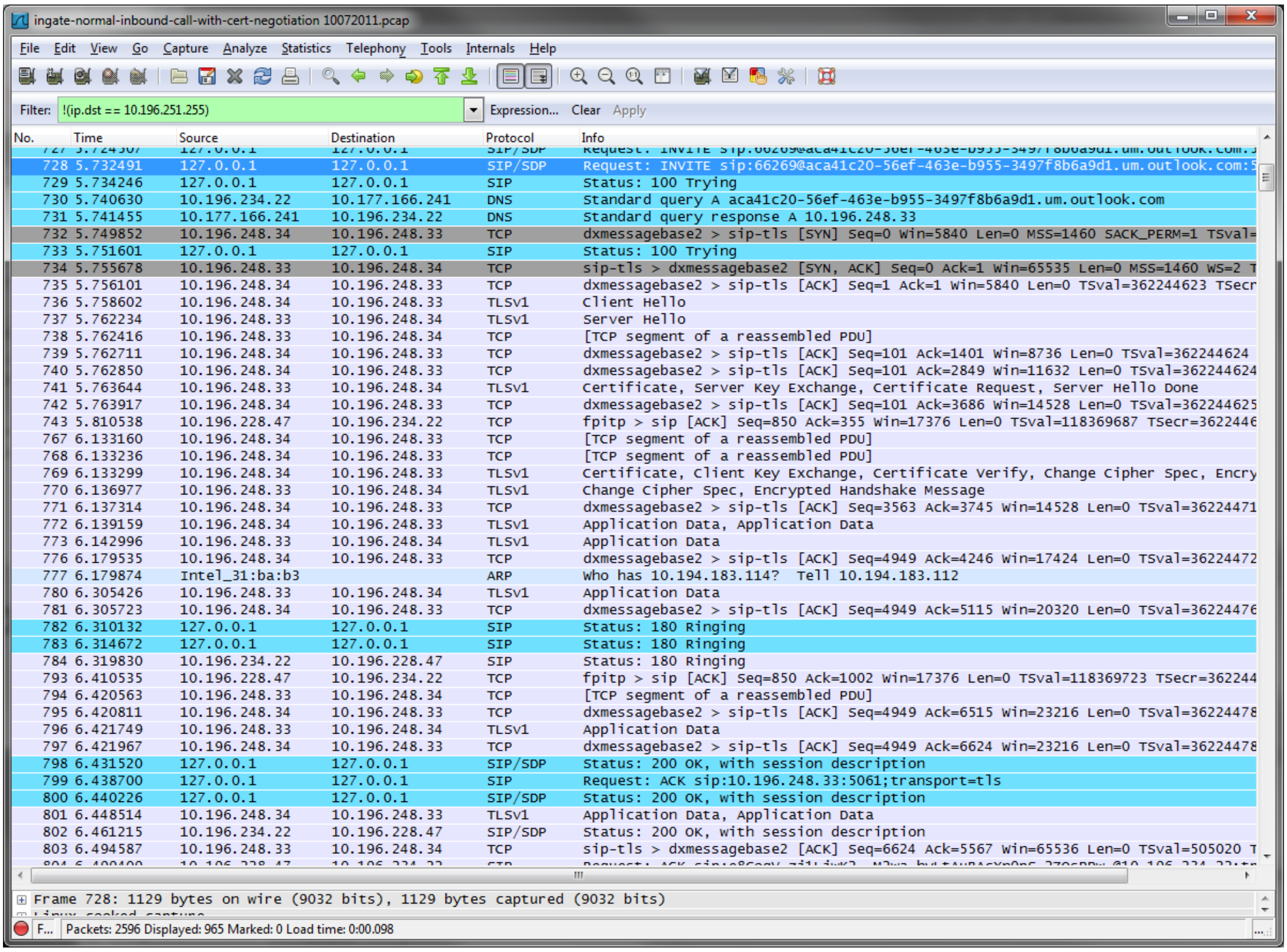
7.1.3 Ingate and Office 365 UM

1) Notice that the packet capture does not show the SIP call flow between the Ingate and the Acme Packet devices. This is because the SIP is being delivered over TLS, and is encrypted.
2) You can see the Ingate “Internal” B2BUA in use, (127.0.0.1) prior to using the TLS connection. This can be used to see what the Ingate sent/received as a packet before/after the encryption.
3) The Acme Packet and Ingate devices negotiate SRTP, or encrypted RTP. Media are streamed between the Ingate and Acme Packet devices. The Ingate SIParator then relays the RTP to the Dialogic gateway.

7.1.4 TLS Transport

TLS requires an initial certificate exchange. The Ingate has a CA-signed root certificate for the Office 365 UM service SBC. All of this is defined in Step 4: Set SBC options to work with Office 365 UM: Configuring SIP Signaling Encryption (TLS).

If the certificate is incorrect for whatever reason (e.g. wrong FQDN for the Ingate device in the certificate subject), the TLS handshake will fail. Within TLS there is no room to overcome incorrect certificates. If the certificate is incorrect, the TLS handshake will fail and the connection will be unable to carry the SIP signaling.



ingate-normal-inbound-call-with-cert-negotiation 10072011.pcap
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: !(ip.dst == 10.196.251.255)
Expression... Clear Apply

```
No.   Time      Source            Destination       Protocol  Info
  728 5.732491  127.0.0.1         127.0.0.1         SIP/SDP   Request: INVITE sip:66269@aca41c20-56ef-463e-b955-3497f8b6a9d1.um.outlook.com:5
  729 5.734246  127.0.0.1         127.0.0.1         SIP       Status: 100 Trying
  730 5.740630  10.196.234.22     10.177.166.241    DNS       Standard query A aca41c20-56ef-463e-b955-3497f8b6a9d1.um.outlook.com
  731 5.741455  10.177.166.241    10.196.234.22     DNS       Standard query response A 10.196.248.33
  732 5.749852  10.196.248.34     10.196.248.33     TCP       dxmessagebase2 > sip-tls [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=
  733 5.751601  127.0.0.1         127.0.0.1         SIP       Status: 100 Trying
  734 5.755678  10.196.248.33     10.196.248.34     TCP       sip-tls > dxmessagebase2 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=2 T
  735 5.756101  10.196.248.34     10.196.248.33     TCP       dxmessagebase2 > sip-tls [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSval=362244623 TSecr
  736 5.758602  10.196.248.34     10.196.248.33     TLSv1     Client Hello
  737 5.762234  10.196.248.33     10.196.248.34     TLSv1     Server Hello
  738 5.762416  10.196.248.33     10.196.248.34     TCP       [TCP segment of a reassembled PDU]
  739 5.762711  10.196.248.34     10.196.248.33     TCP       dxmessagebase2 > sip-tls [ACK] Seq=101 Ack=1401 Win=8736 Len=0 TSval=362244624
  740 5.762850  10.196.248.34     10.196.248.33     TCP       dxmessagebase2 > sip-tls [ACK] Seq=101 Ack=2849 Win=11632 Len=0 TSval=362244624
  741 5.763644  10.196.248.33     10.196.248.34     TLSv1     Certificate, Server Key Exchange, Certificate Request, Server Hello Done
  742 5.763917  10.196.248.34     10.196.248.33     TCP       dxmessagebase2 > sip-tls [ACK] Seq=101 Ack=3686 Win=14528 Len=0 TSval=362244625
  743 5.810538  10.196.228.47     10.196.234.22     TCP       fpitp > sip [ACK] Seq=850 Ack=355 Win=17376 Len=0 TSval=118369687 TSecr=3622446
  767 6.133160  10.196.248.34     10.196.248.33     TCP       [TCP segment of a reassembled PDU]
  768 6.133236  10.196.248.34     10.196.248.33     TCP       [TCP segment of a reassembled PDU]
  769 6.133299  10.196.248.34     10.196.248.33     TLSv1     Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encry
  770 6.136977  10.196.248.33     10.196.248.34     TLSv1     Change Cipher Spec, Encrypted Handshake Message
  771 6.137314  10.196.248.34     10.196.248.33     TCP       dxmessagebase2 > sip-tls [ACK] Seq=3563 Ack=3745 Win=14528 Len=0 TSval=36224471
  772 6.139159  10.196.248.34     10.196.248.33     TLSv1     Application Data, Application Data
  773 6.142996  10.196.248.33     10.196.248.34     TLSv1     Application Data
  776 6.179535  10.196.248.34     10.196.248.33     TCP       dxmessagebase2 > sip-tls [ACK] Seq=4949 Ack=4246 Win=17424 Len=0 TSval=36224472
  777 6.179874  Intel_31:ba:b3                      ARP       Who has 10.194.183.114?  Tell 10.194.183.112
  780 6.305426  10.196.248.33     10.196.248.34     TLSv1     Application Data
  781 6.305723  10.196.248.34     10.196.248.33     TCP       dxmessagebase2 > sip-tls [ACK] Seq=4949 Ack=5115 Win=20320 Len=0 TSval=36224476
  782 6.310132  127.0.0.1         127.0.0.1         SIP       Status: 180 Ringing
  783 6.314672  127.0.0.1         127.0.0.1         SIP       Status: 180 Ringing
  784 6.319830  10.196.234.22     10.196.228.47     SIP       Status: 180 Ringing
  793 6.410535  10.196.228.47     10.196.234.22     TCP       fpitp > sip [ACK] Seq=850 Ack=1002 Win=17376 Len=0 TSval=118369723 TSecr=362244
  794 6.420563  10.196.248.33     10.196.248.34     TCP       [TCP segment of a reassembled PDU]
  795 6.420811  10.196.248.34     10.196.248.33     TCP       dxmessagebase2 > sip-tls [ACK] Seq=4949 Ack=6515 Win=23216 Len=0 TSval=36224478
  796 6.421749  10.196.248.33     10.196.248.34     TLSv1     Application Data
  797 6.421967  10.196.248.34     10.196.248.33     TCP       dxmessagebase2 > sip-tls [ACK] Seq=4949 Ack=6624 Win=23216 Len=0 TSval=36224478
  798 6.431520  127.0.0.1         127.0.0.1         SIP/SDP   Status: 200 OK, with session description
  799 6.438700  127.0.0.1         127.0.0.1         SIP       Request: ACK sip:10.196.248.33:5061;transport=tls
  800 6.440226  127.0.0.1         127.0.0.1         SIP/SDP   Status: 200 OK, with session description
  801 6.448514  10.196.248.34     10.196.248.33     TLSv1     Application Data, Application Data
  802 6.461215  10.196.234.22     10.196.228.47     SIP/SDP   Status: 200 OK, with session description
  803 6.494587  10.196.248.33     10.196.248.34     TCP       sip-tls > dxmessagebase2 [ACK] Seq=6624 Ack=5567 Win=65536 Len=0 TSval=505020 T

Frame 728: 1129 bytes on wire (9032 bits), 1129 bytes captured (9032 bits)
Packets: 2596 Displayed: 965 Marked: 0 Load time: 0:00.098
```

7.1.5 Typical TLS Handshake

1) TLS starts with a TCP SYN request, and SYN ACK response from the far end
2) There is a TLSv1 Client Hello followed by a Server Hello response from the far end
3) The certificates are exchanged, Server Key Exchange followed by the Client Key Exchange.
4) Success comes by way of a TLS handshake message.

7.1.6 Failure of TLS Handshake

Failure of TLS Transport come is a variety of forms:

1) Wrong certificate Type installed on Ingate. The Device Cert is installed in the “Private” certificate store, where the intermediate certificate is installed in the CA certificate store.
2) Wrong FQDN in the CA certificate. The Ingate SIParator must be able to identify the Office 365 Exchange Online service by the service’s fully qualified domain name (FQDN).
3) Likewise the Office 365 IM – Acme Packet must have the correct FQDN for the Ingate. 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`)
4) Most often, if TLS is not working, an incorrect certificate is being used. The process of establishing TLS, i.e. the handshake and the certificate exchange are very much standard. But validating the Cert, should there be an error in the certificate there is little to no leeway for negotiation, and discovery of the nature of the error within the certificate needs to be investigated.