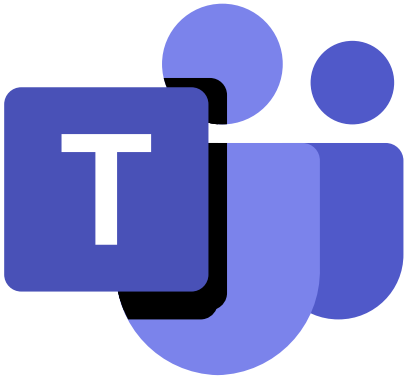
EDUCRONIX

TELECOMM SKILLS AT YOUR HANDS

Setting up Ingate's

SIParator® / Firewall®

For



Microsoft Teams

For Ingate SIParators using software release 6.3.3 or later

Revision 1.3

January 2022

Ingate SIParator®/Firewall® for Microsoft Teams

Table of Contents

1 Minimum Requirements

1.1 SIParator Version

This document applies to :

- SIParator/Firewall Version 6.3.1 or later.
- All Ingate Models, physical and virtual (AWS, Azure, Google Cloud and OpenStack etc).

1.2 Ingate Licensing

SIP Trunk Licensing with enough CCS depending on the number of simultaneous calls to be routed using Direct Route to/from ITSP

Additional Trunk Licenses with shared or additional CCS to route traffic to an IP PBX if necessary.

For additional license needs, connect with your Ingate representative.

1.3 Office Tenant Account

A Microsoft Office (Office 365) Tenant account with appropriate licensing to include Cloud PBX Service is needed. Details here:

- https://docs.microsoft.com/en-us/office365/servicedescriptions/teams-service-description.
- https://docs.microsoft.com/en-us/microsoftteams/teams-add-on-licensing/microsoft-teams-add-on-licensing?tabs=small-business

1.4 Domain ownership

A Domain must be properly set up and associated with the Office Account. For more details review:

https://docs.microsoft.com/en-us/microsoft-365/admin/setup/add-domain?view=o365-worldwide

1.5 FQDN/Public IP for the SBC

A specific Public IP address and an FQDN under your domain is needed for the SBC.

FQDN must be published in public DNS.

1.6 Public Trusted certificate.

An SSL Certificate, properly signed by a Trusted CA will be needed for the SBC. For more details about the certificate see here: https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#public-trusted-certificate-for-the-sbc

1.7 Firewall ports and IP addresses properly configured.

Details here: https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#microsoft-365-office-365-and-office-365-gcc-environments

For more details please visit: https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan

1.8 Office 365 infrastructure prerequisites

This is dynamic information, likely to change, and is presented whole, in an attempt to be helpful. Not all of this information may be relevant or applicable, as Microsoft continually folds some of the below steps into their web based GUI, making the below steps unnecessary. Some of the branding regards the older Skype for Business, which Microsoft are moving away from.

In earlier integrations with MS Teams, there were a few PowerShell commands necessary.

1.8.1 Pair your SBC with the Direct Routing Service (DRS)

```
# New-CsOnlinePSTNGateway -Fqdn <SBC FQDN> -SipSignallingPort <SBC SIP Port> -
MaxConcurrentSessions <SBC Max Concurrent Calls> -Enabled $true
```

e.g.

```
# New-CsOnlinePSTNGateway -Fqdn sbc.mycompany.com -SipSignallingPort 5061 -
MaxConcurrentSessions 10 -Enabled $true
```

To e.g. change the SIP port

```
# Set-CsOnlinePSTNGateway -Identity sbc.mycompany.com -SIPSignallingPort 5067
```

To e.g. verify the SBC is correctly set

```
# Get-CsOnlinePSTNGateway -Identity sbc.mycompany.com

Identity                        : sbc.mycompany.com

Fqdn                            : sbc.mycompany.com

SipSignallingPort               : 5061

FailoverTimeSeconds             : 10

ForwardCallHistory              : False

ForwardPai                      : False

SendSipOptions                  : True

MaxConcurrentSessions           : 100

Enabled                         : True

MediaBypass                     : False
```

```
GatewaySiteId                     :

GatewaySiteLbrEnabled             : False

FailoverResponseCodes             : 408,503,504

GenerateRingingWhileLocatingUser  : True

PidfLoSupported                   : False

MediaRelayRoutingLocationOverride :

ProxySbc                          :

BypassMode                        : None
```

1.8.2 Configure specific users for DRS

Roughly:

- Create a user in Office 365. Assign a phone system license.
- Ensure that the user is homed in Skype for Business Online.
- Configure the phone number and enable enterprise voice and voicemail.
- Configure voice routing. The route is automatically validated.

```
# Set-CsUser -Identity "<Username>" -EnterpriseVoiceEnabled $true -
HostedVoiceMail $true -OnPremLineURI tel:<E.164 phone number>
```

e.g.

```
# Set-CsUser -Identity "john@mycompany.com" -EnterpriseVoiceEnabled $true -
HostedVoiceMail $true -OnPremLineURI tel:+13105550001
```

To verify:

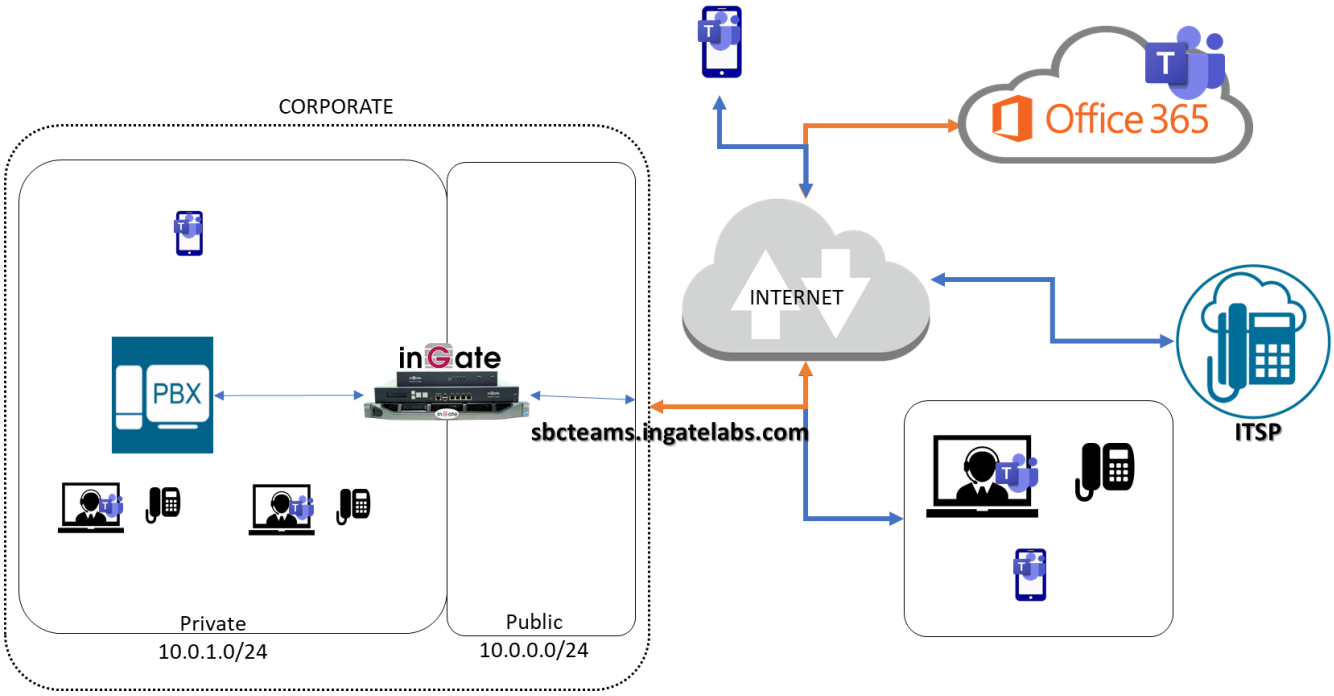
```
# Get-CsOnlineUser -Identity " john@mycompany.com " | fl RegistrarPool

RegistrarPool : sippoolCO24A05.infra.lync.com
```

2 SIParator configuration

The next subsections explain in detail how to configure your SIParator SBC in typical use case scenarios.

2.1 Topology with SIParator in the DMZ, IPPBX on LAN and ITSP on WAN



In this scenario we have users associated to an existing third-party IPPBX (It could be plain analog extensions, proprietary phones, SIP phones, etc.).

Some user could have also a Teams client extension associated, or even users may have only Teams.

They can be local to Corporate offices, in the LAN or even in remote offices (They can be using the SBC to support remote IPPBX users, or any other IPPX supported mechanism for remote extensions).

2.1.1 Requirements

A Public IP address allocated to the SBC (Via DMZ mapping, or directly assigned to the SBC external interface).

An FQDN resolving to the Public IP, and also used as the SIP domain for Teams users (e.g. user@sbc.domain.com)

A Public Certificate, issued by one of the MS supported CA as explained here: https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#public-trusted-certificate-for-the-sbc. This certificate will be installed in the SBC as a Server Private Certificate.

Baltimore CA Root Certificates as required by Teams shall be installed on the SBC. It is necessary for mTLS connections with sip.pstnhub.microsoft.com

You can use either of these links to download the certificate:

https://cacert.omniroot.com/bc2025.pem

https://cacert.omniroot.com/bc2025.crt

2.1.2 SBC Domain

The SBC Domain Must be one registered in the "Domains" for the tenant account. The name must be like:

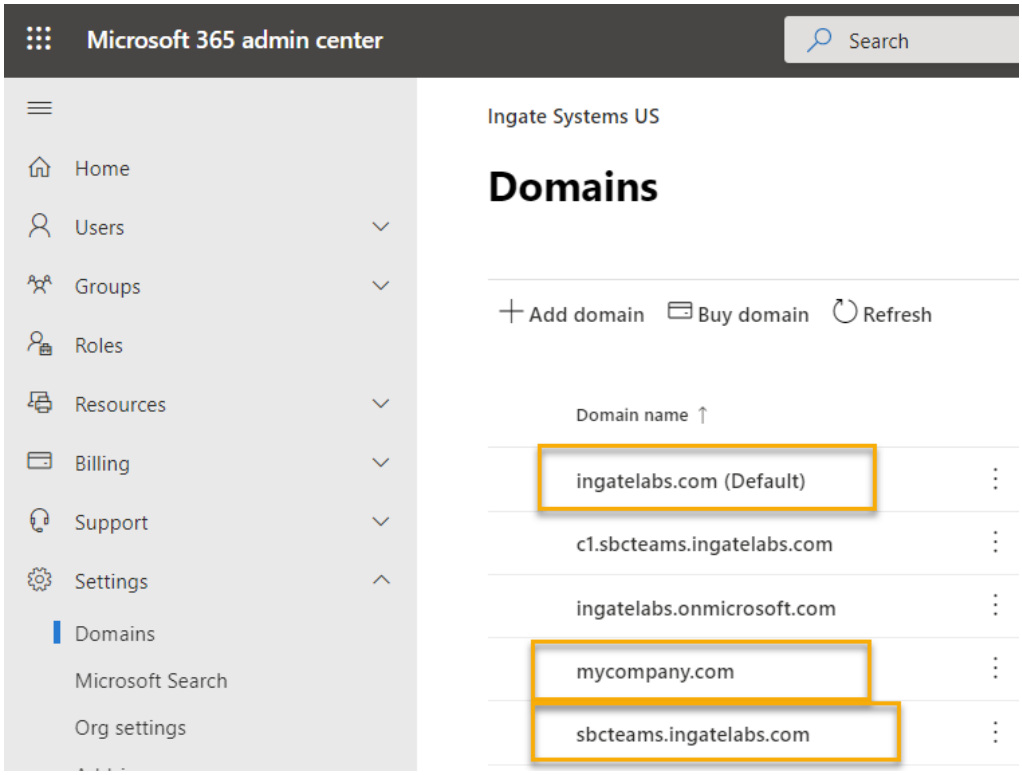
<anyname>.tenant.com, where tenant.com is your domain.

Some examples:

- For domain: "mydomain.com"
  - sbc.mydomain.com (Valid)
  - sip1sbc.mydomain.com (Valid)
  - site1.sbc.mydomain.com (wrong!)
- For domain: "mygreatcompany.biz"
  - voice.mygreatcompany.biz (Valid)
  - mainsbc.mygreatcompany.biz (Valid)
  - site5.sbc.mygreatcompany.biz (wrong!)
- For domain: "ingatelabs.com"
  - sbcteams.ingatelabs.com (Valid)
  - sbc53.ingatelabs.com (Valid)
  - sbc.teams.ingatelabs.com (wrong!)

Please note that users could be associated to any domain, as far as the domain is registered under the tenant account. For instance, user ***mike@mydomain.com*** can use direct route with an SBC named ***sbcteams.ingatelabs.com*** as long as both domains are registered for this tenant.

It should look like this in your Office Admin Domain dashboard:

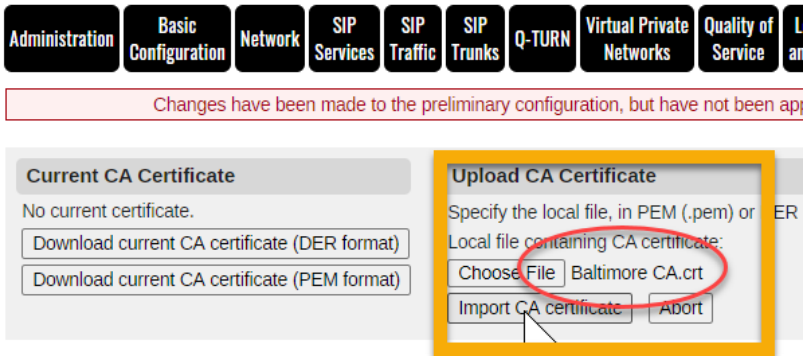


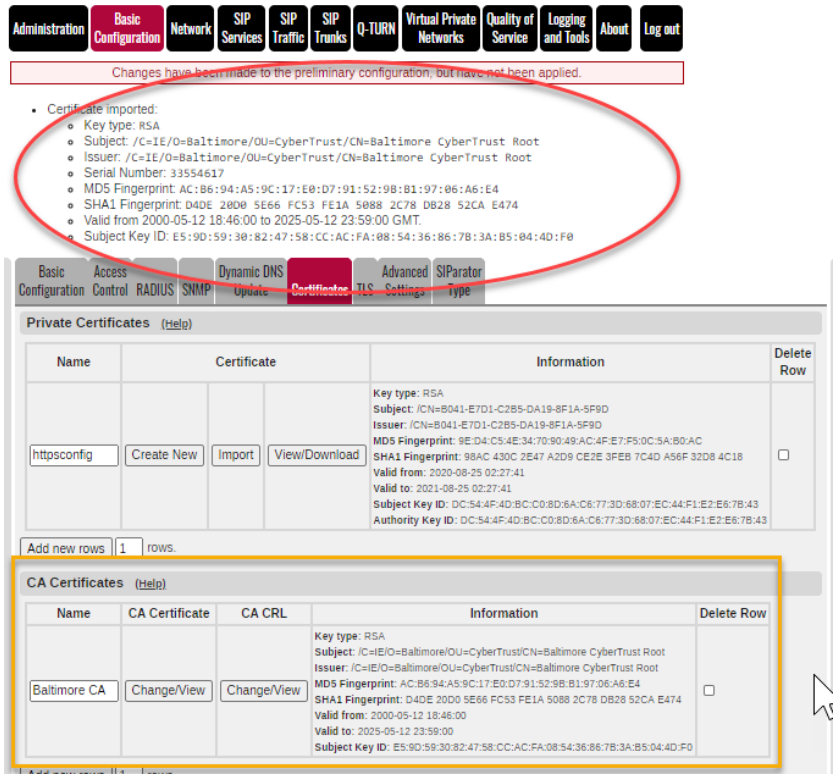
For the purpose of this document we use

sbcteams.ingatelabs.com → 34.195.120.56

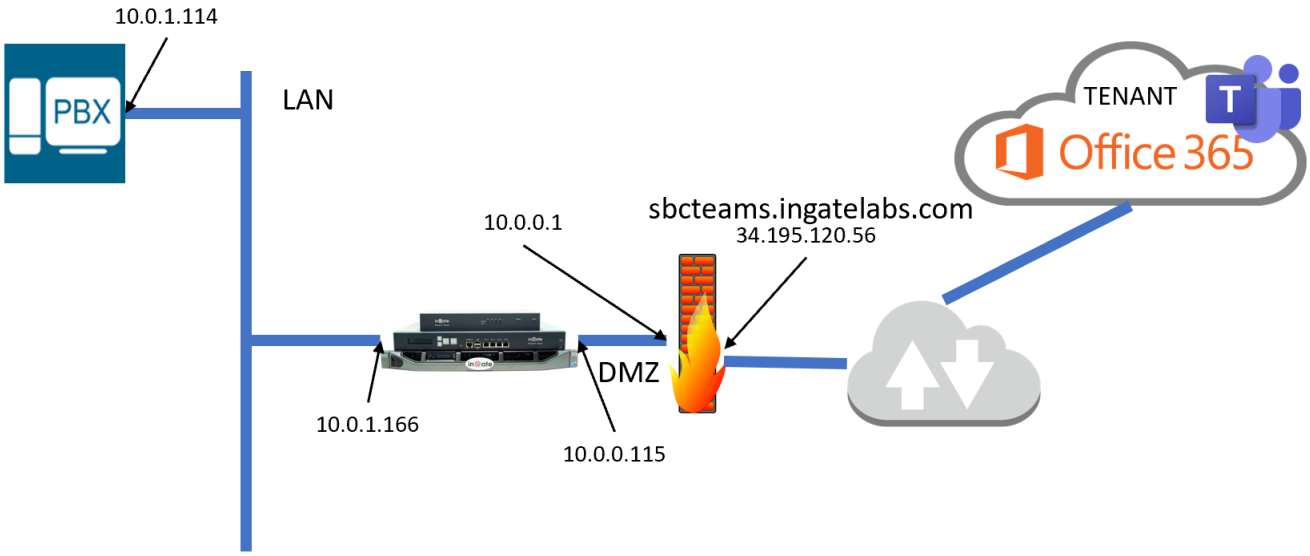
2.1.3 Deploy the Baltimore Certificate

Import the certificate under Basic Configuration→Certificates→ CA Certificate

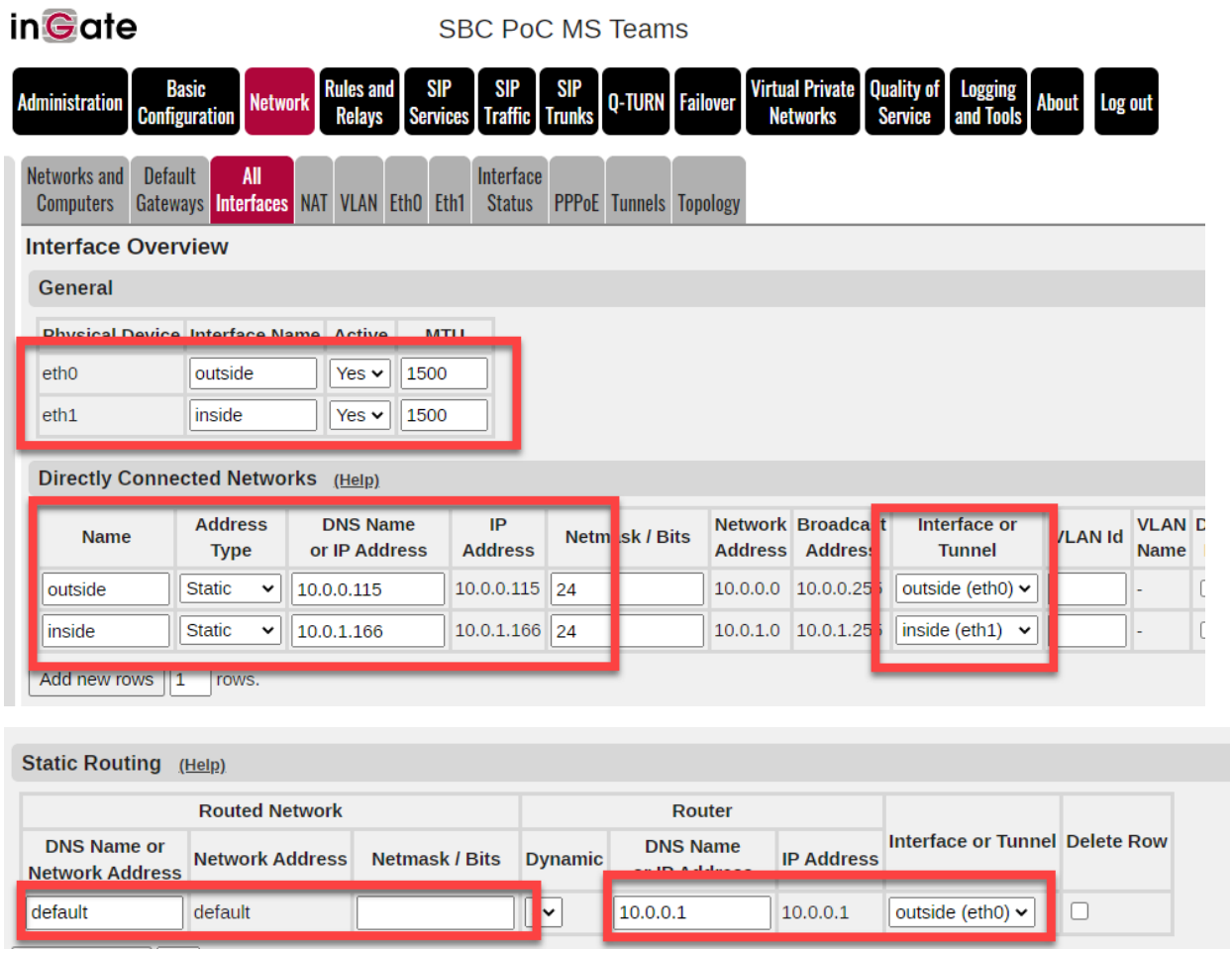




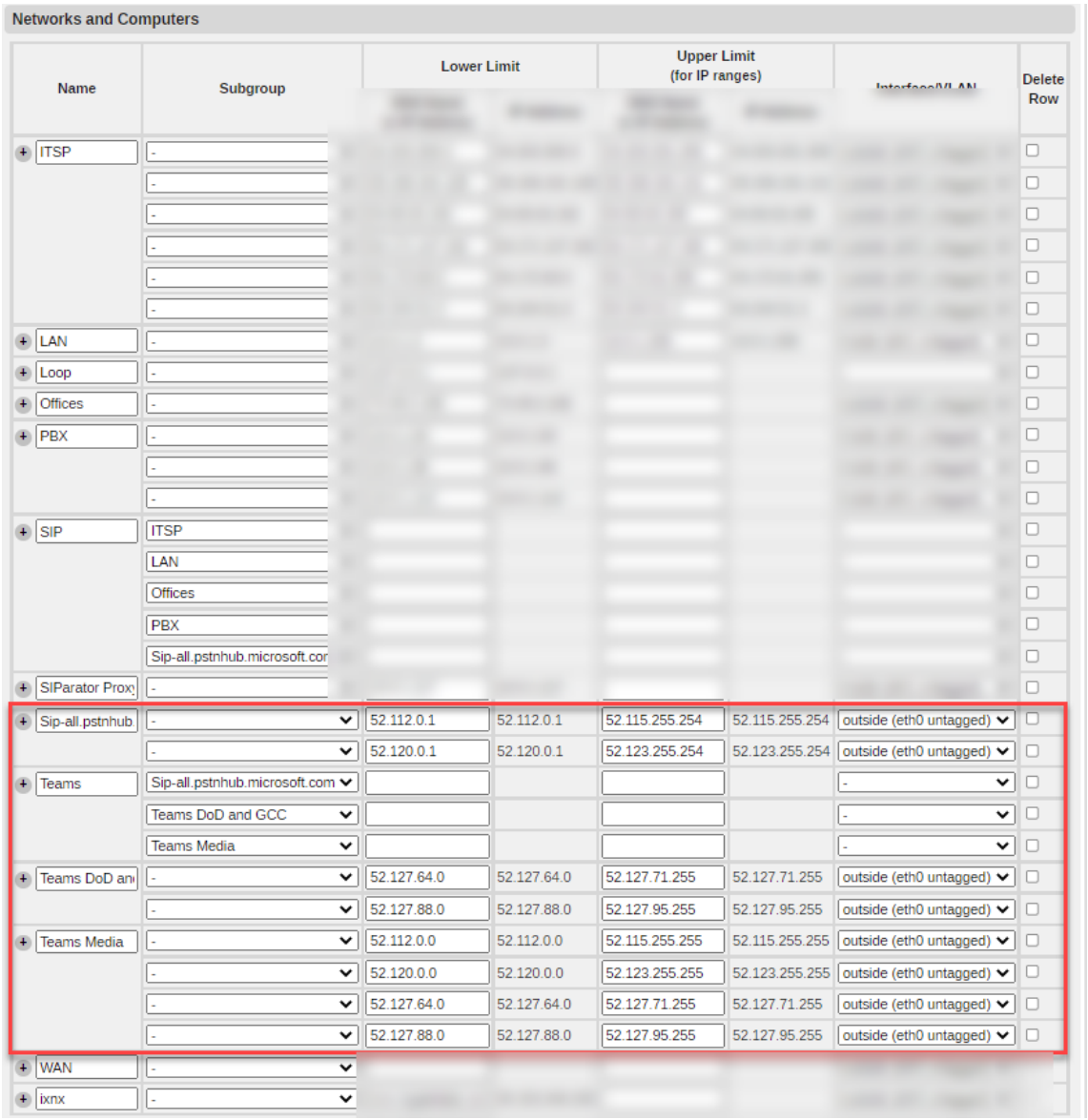
2.1.4 SIParator Network configuration



Here, eth0 will be in the DMZ (outside) and eth1 will be on the LAN (inside). Network configuration interfaces and default gateway (10.0.0.1) will look like this:



We will create a set of network names to facilitate configuration. Under Networks → Networks and Computers:



NOTE: it is always a good practice to review latest information available from Microsoft regarding Ips assigned for signaling and media and adjust accordingly (Plan Direct Routing - Microsoft Teams | Microsoft Docs)

- **ITSP**: all IP addresses (Signaling and Media) provided by the ITSP from which traffic can originate
- **LAN**: Local subnet
- **Loop**: name to be used to refer to Local Loop in the SBC.
- **MS Media**: Microsoft's range of IPs used for Media. A.k.a. Media Servers IPs.
- **PBX**: IPPBX – also used to route calls between Teams and PBX as well as the ITSP.
- **Teams Bypass Media**: IP ranges used by Teams for Bypass media and media path optimization

- **Teams DoD**: IP Microsoft IPs to provide service to DoD; the equivalent of Microsoft SIP Hubs but for DoD
- **WAN**: To refer to any traffic on the Internet
- **sip-all.pstnhub.microsoft.com**: IP addresses used by Teams to originate or receive SIP signaling
- **Teams**: A name to group together all IPs belonging to Microsoft (sip-all.pstnhub, DoD, MS media, Media Bypass) – a security domain, if you will.

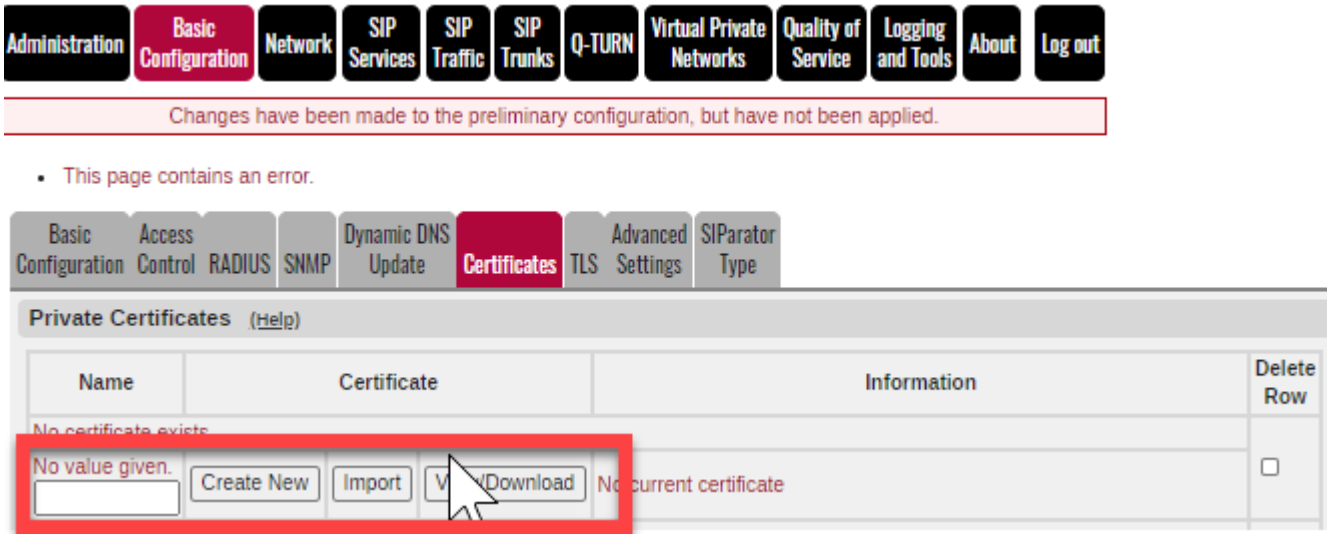
2.1.5 SIParator SIP Encryption configuration

As Teams will use TLS signaling, we need to load a Trusted CA certificate for the SIParator to use for its Private certificate.

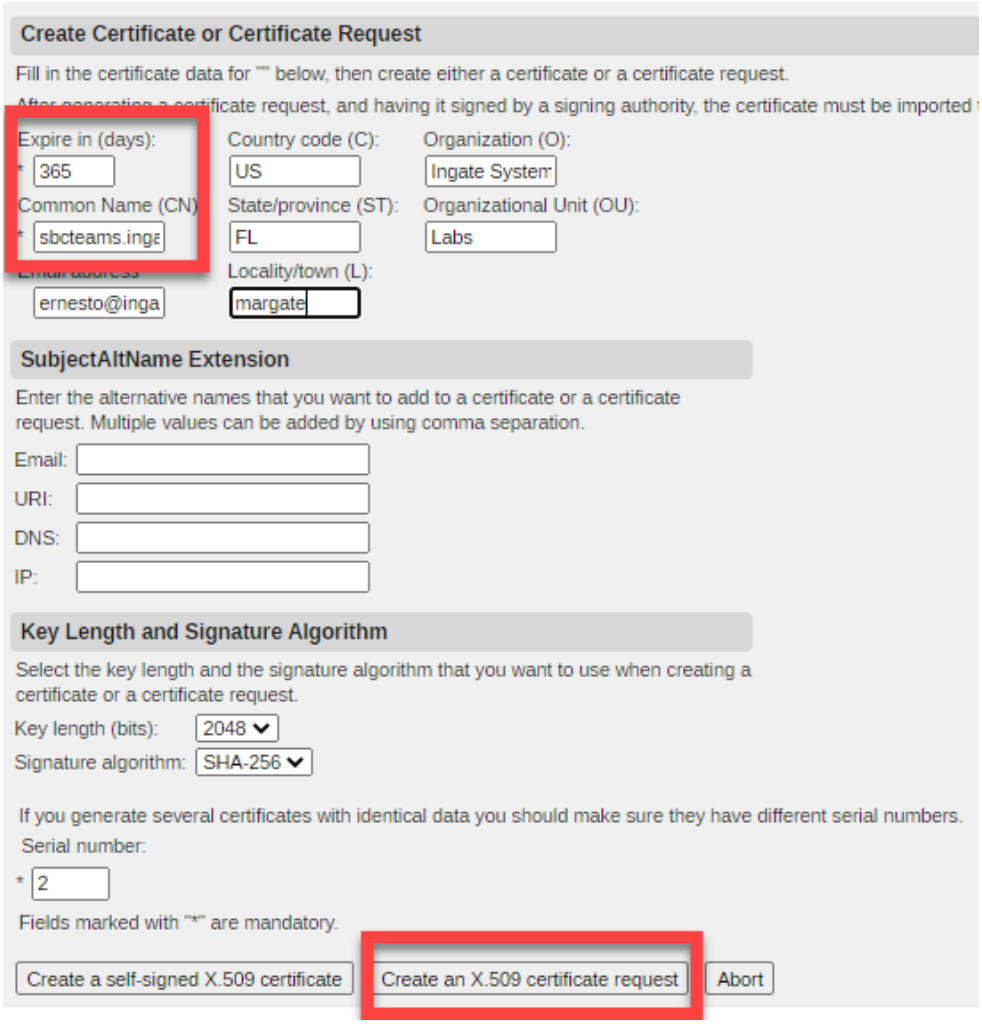
You should obtain a certificate signed by a trusted CA based on Microsoft recommendations (https://docs.microsoft.com/en-us/microsoftteams/direct-routing-plan#public-trusted-certificate-for-the-sbc).

2.1.5.1 Create a CSR

You can create a Certificate Signing Request (CSR) directly from the Ingate GUI:



Just add a row on the Private Certificates Section, assign a name and then click on Create New button.



Complete the form and make sure you define the expiration time you need for this certificate to be valid, and more importantly, fill in the **SubjectAltName (or sAN) URI** field, and optionally the CN (Common Name) of the certificate request with the FQDN of the SBC (sbcteams.ingatelabs.com in our case).

Choose Create X.509 certificate request (a CSR), a CSR will be generated.

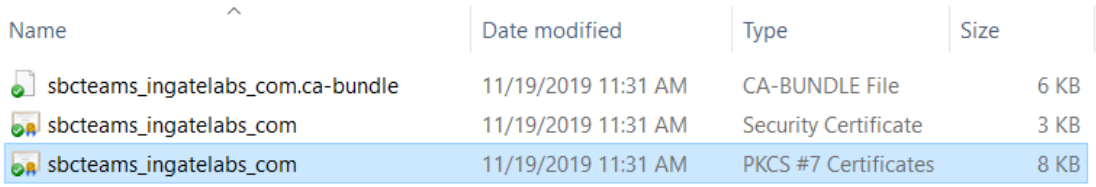
Note: Standards do not recognize the use of domain names in the CN field, only in the **sAN DNS** field.

Note: SIP standards do not recognize wildcards (*.) in either field.

2.1.5.2 Provide CSR to CA – get a valid certificate

Download this CSR: it will be used to by your chosen CA for them to produce the signed certificate.

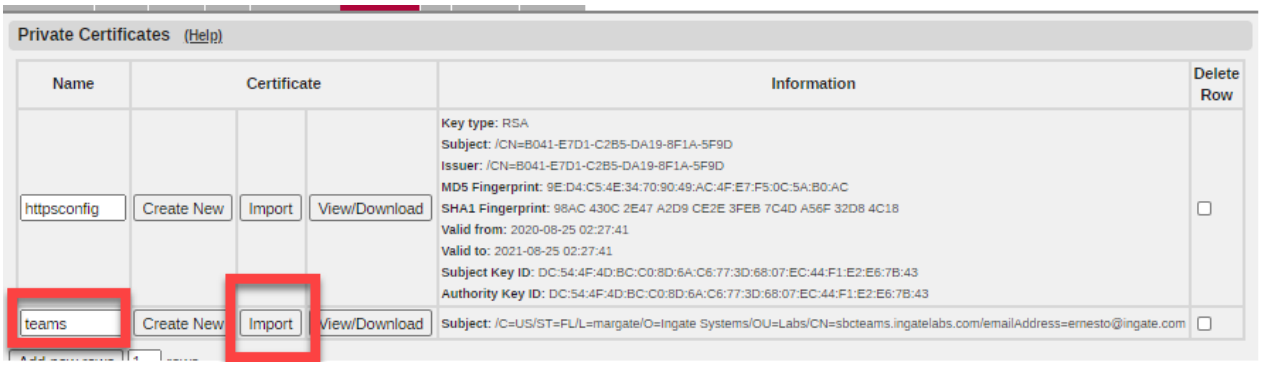
Once you obtain the signed certificate, you'll get more than one file, sometimes in a chain including their CA public half. It might look something like this:



Usually signed certificate in two formats (DER, PKCS7 in this case) and a CA Bundle.

2.1.5.3 Import your signed certificate

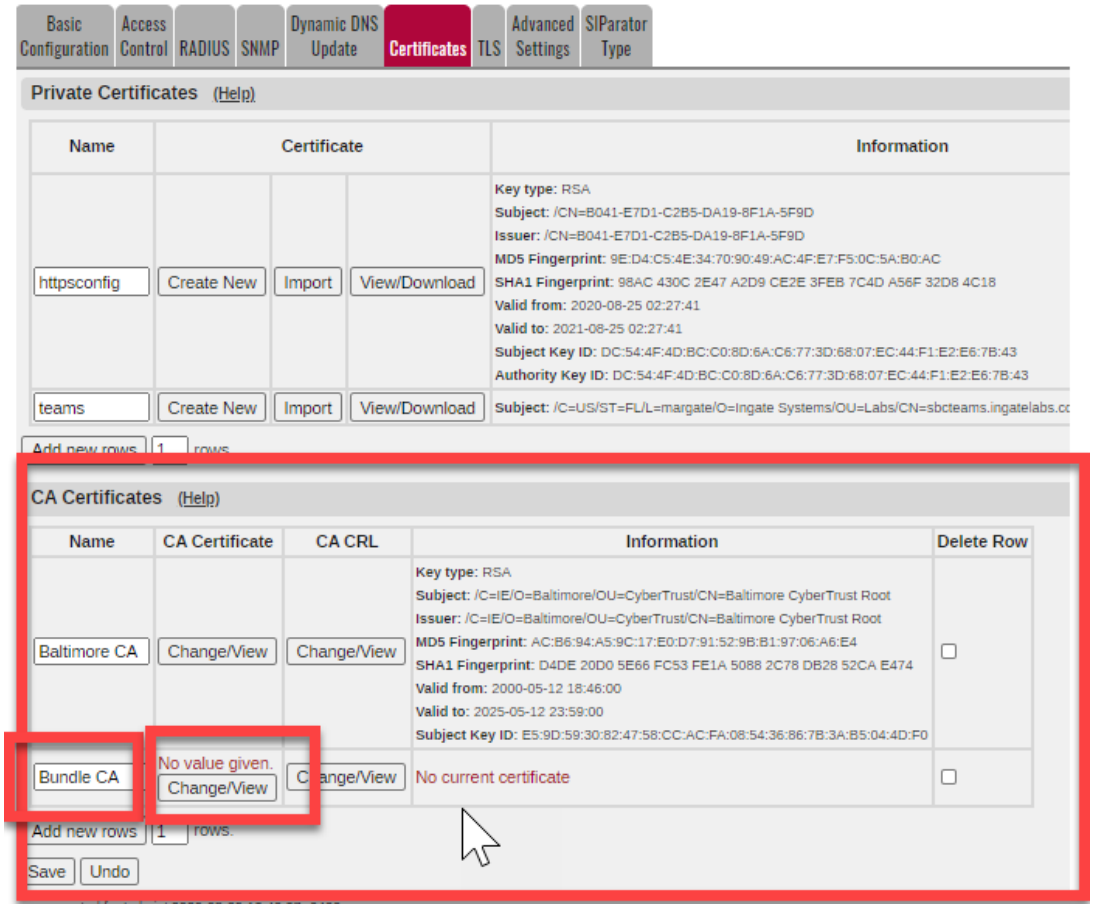
You'll need to import the signed certificate into the entry you created for the CSR:



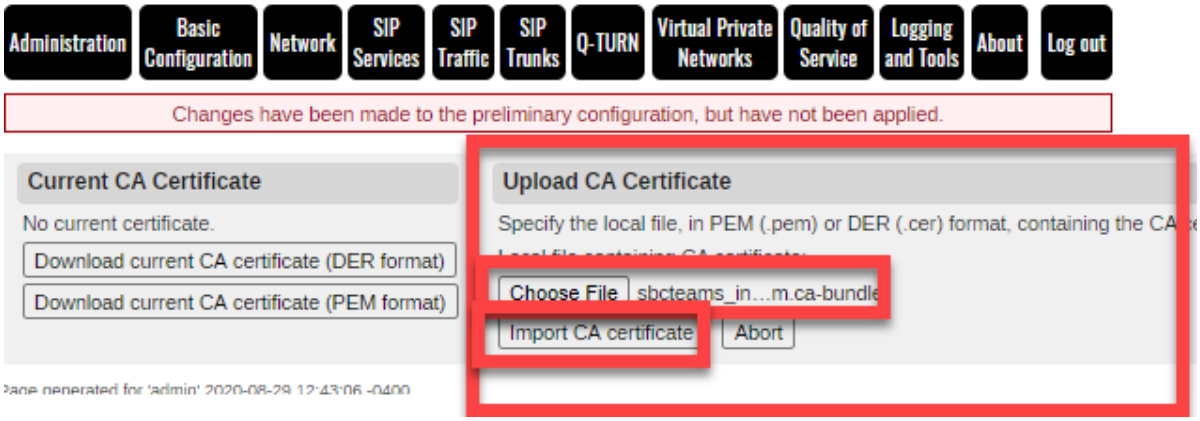
Select the file and click Import signed certificate.

2.1.5.4 Import the signing CA

Now, you will need to add the Bundle CA certificate to the SIParator, the CA public certificate which signed your CSR:

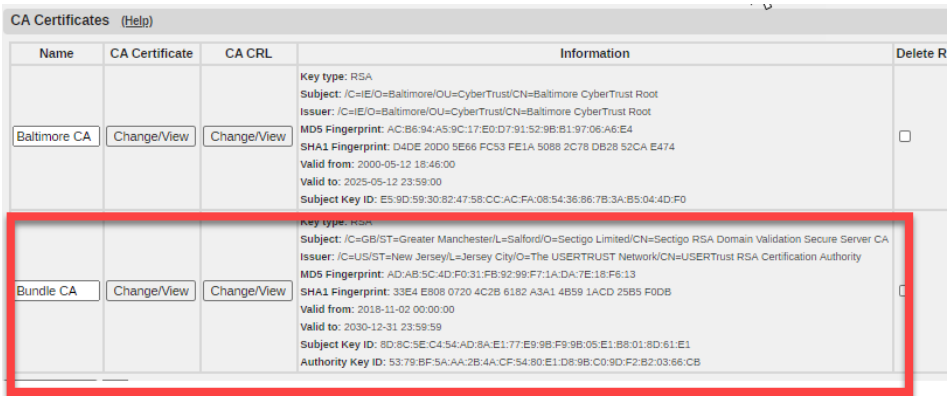


Add a new row in the CA Certificates section, assign a name and click on Change/View button.



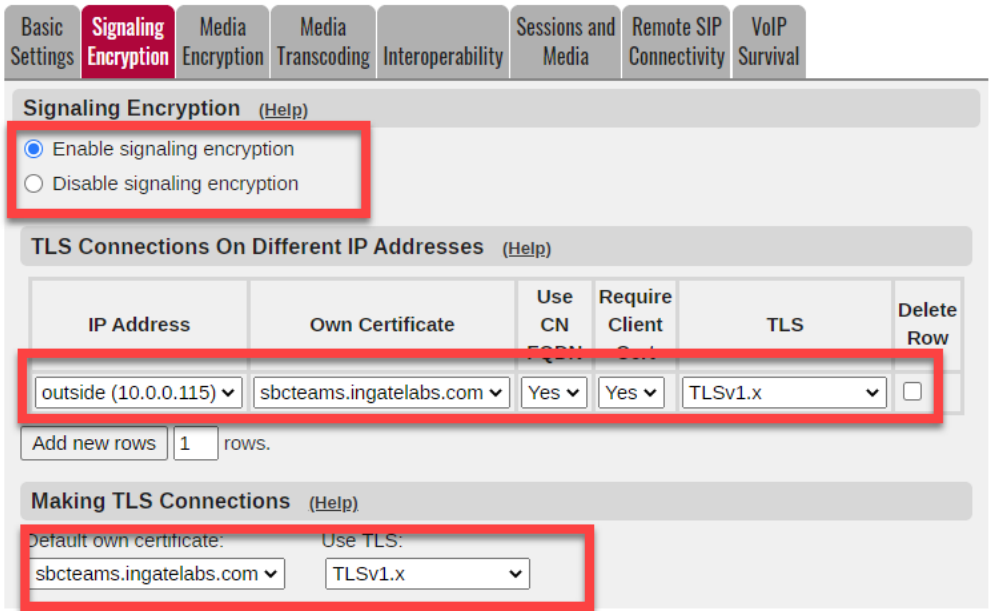
Choose the Bundle file provided by the Trusted CA you used for signing the certificate and click on import certificate.

The CA certificate should show up in the CA Certificates section:



2.1.5.5 Configure SIP TLS with the certificates

At this point you are ready to set up TLS signaling on the SIParator. Under SIP Services, go to Signaling Encryption



Enable signaling encryption

Add a row on **TLS Connections On Different IP addresses**, select the outside interface.

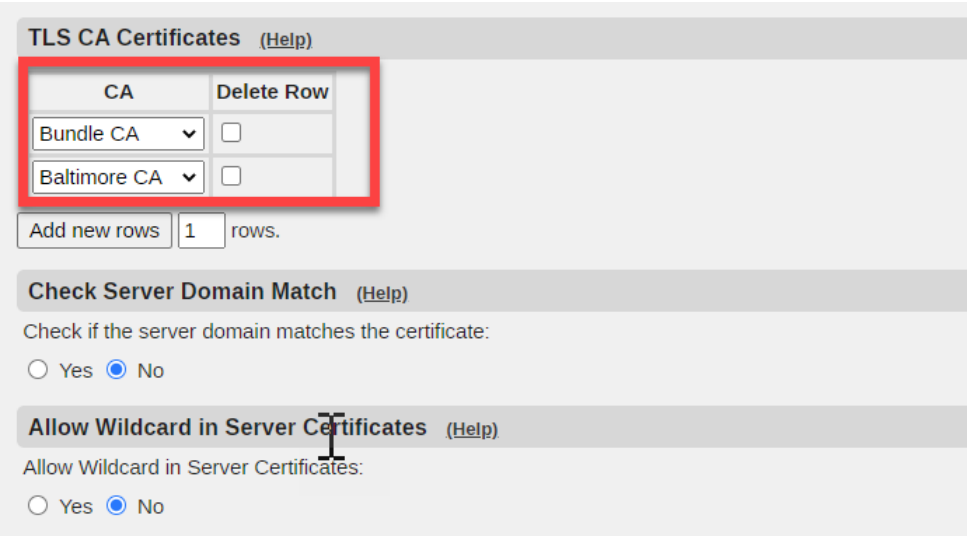
Select the new certificate you just got signed and loaded.

Select Yes on **Use CN FQDN** (with this, the SBC uses the certificate CA/sAN URI as the FQDN in SIP URI headers)

Select Yes on **Require Client Certificate** (this enables mTLS)

Select TLSv1.x in the TLS column.

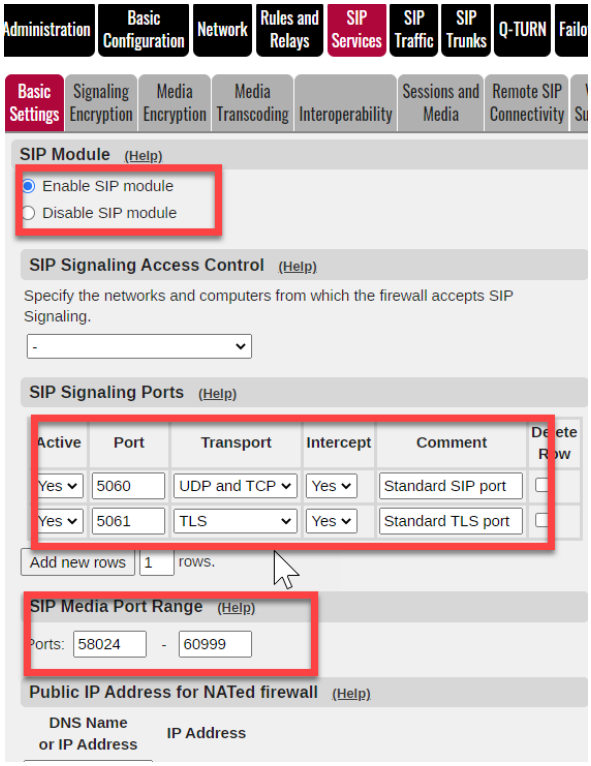
Under "**Making TLS connections**", select the same certificate used in the previous steps.



Under "**TLS CA Certificates**" add the two recently added CA Certificates (Baltimore CA and Bundle CA).

2.1.6 Configure SIP Signaling

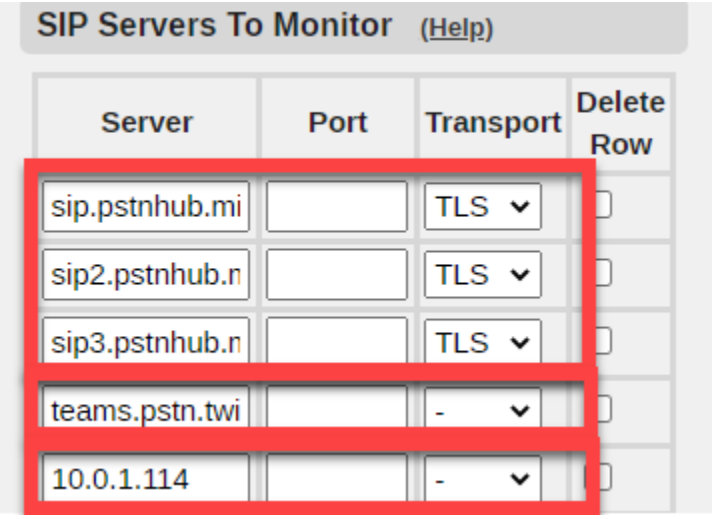
In this section, enable UDP ports to be used with your IPPBX as well as the ITSP, and TLS to be used with Teams (if not already used with your ITSP).



Enable the SIP module

Under **SIP signaling ports**, make active port 5060 for TCP and UDP, as well as 5061 for TLS. In both cases select Intercept "Yes"

Keep the default **Media Port Range**.



Add to **SIP Monitor** FQDNs for Microsoft SIP hubs, the carrier domain (Trunk provided by the ITSP) and the IPPBX on 10.0.1.114.

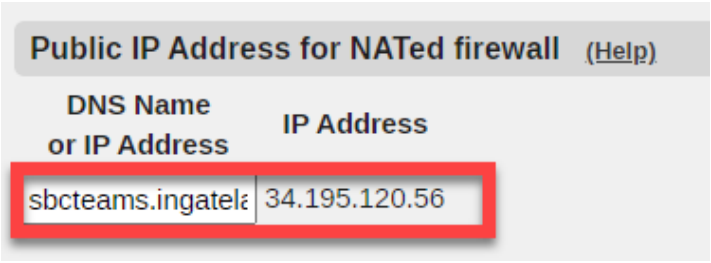
Note: teams.pstn.tw…. is our ISTP Trunk domain, that will be explained later in this document.

Microsoft SIP hubs are:

- sip.pstnhub.microsoft.com
- sip2.pstnhub.microsoft.com
- sip3.pstnhub.microsoft.com

The IPPBX is 10.0.1.114

This will keep the status updated for each sip endpoint using SIP OPTIONS keep-alive requests.



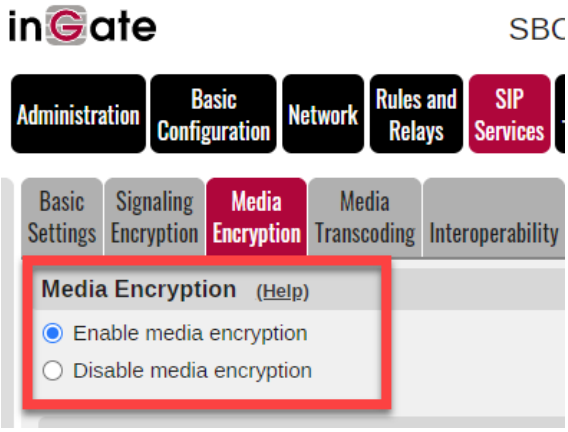
In this use-case scenario, the SIParator external interface is connected to a private DMZ, we add the external public IP address, which corresponds to the SBC FQDN. In our case:

sbcteams.ingatelabs.com.

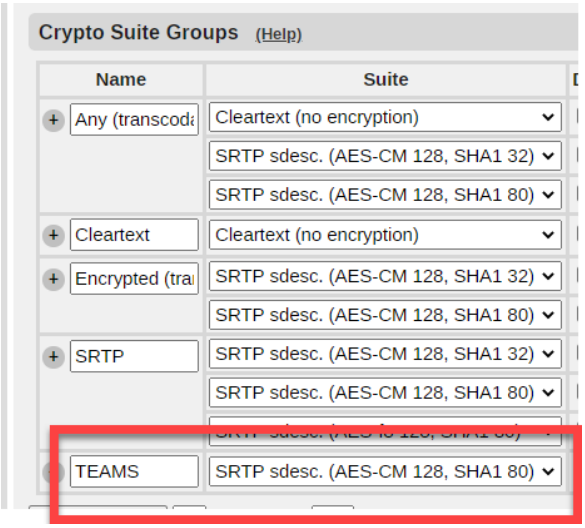
Enter the FQDN or the Public IP.

2.1.7 Configure Media Encryption

First, under SIP Services → Media Encryption:



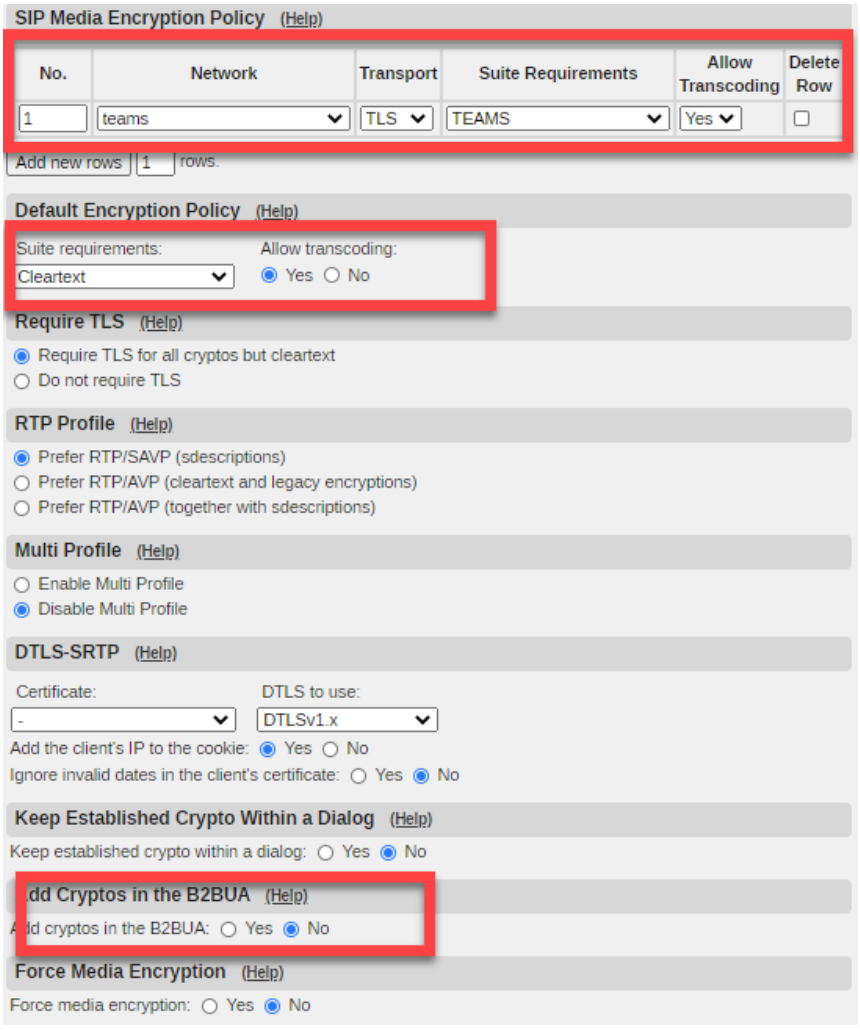
Enable **Media Encryption**



Create a single **Crypto Suite Group** for teams as shown.

There are plans in the future to support DTLS/SIPS. Once Microsoft announces it, it will be very easy to change configuration here.

Assuming Media Encryption happens only between the SBC and Teams Media Servers, define it like this:



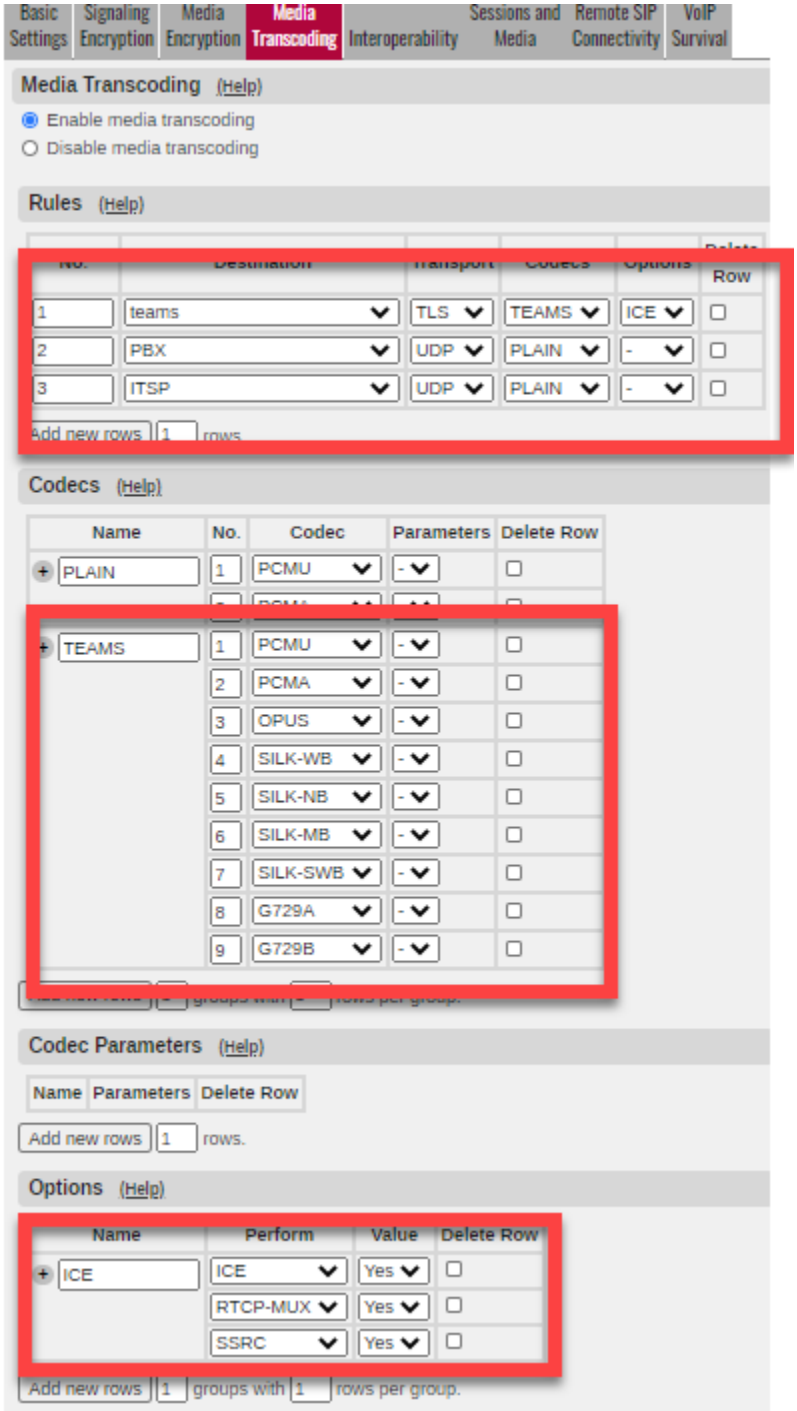
Add a **Media Encryption Policy** to apply the TEAMS suite group created above.

Allow **transcoding**

Default encryption: Cleartext for all other cases. Allow transcoding.

Make sure you disable **Add Cryptos in the B2BUA.**

2.1.8 Configure Media Transcoding



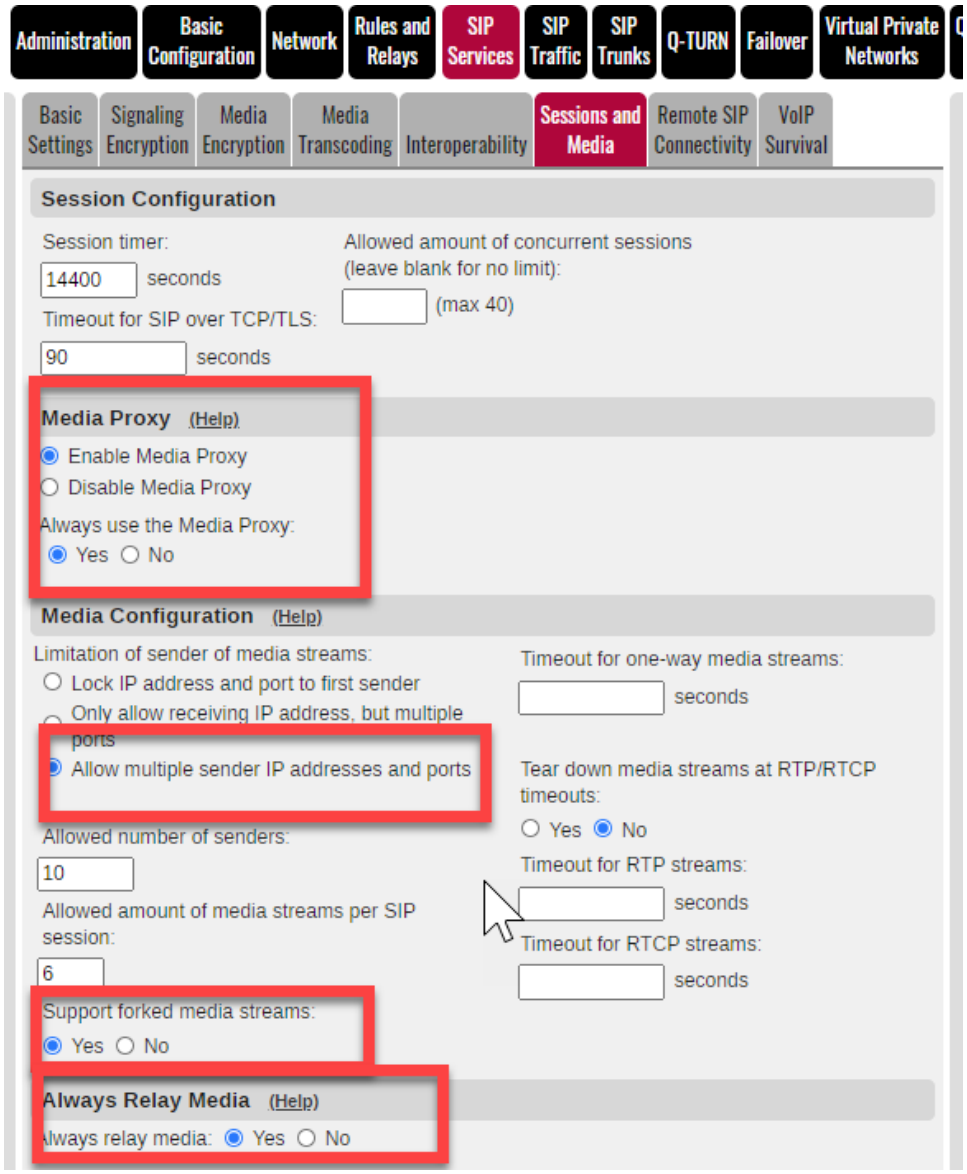
Enable Media Transcoding.

Define rules for teams media, PBX and the ITSP based on codecs supported by each one.

Teams Supported **Codecs**, include SILK (Preferred by Teams client), OPUS for WebRTC Media Bypass. Also G711 and G729 are supported.

Name an **Options** group **ICE** as configured at the bottom. This enables ICE-Lite (RFC5245) and transport relay in the client Support, SRTCP Port multiplexing and SSRC (RFC3550) Multiple Synchronization Sources.

2.1.9 Other Media related configuration



Enable Media Proxy.

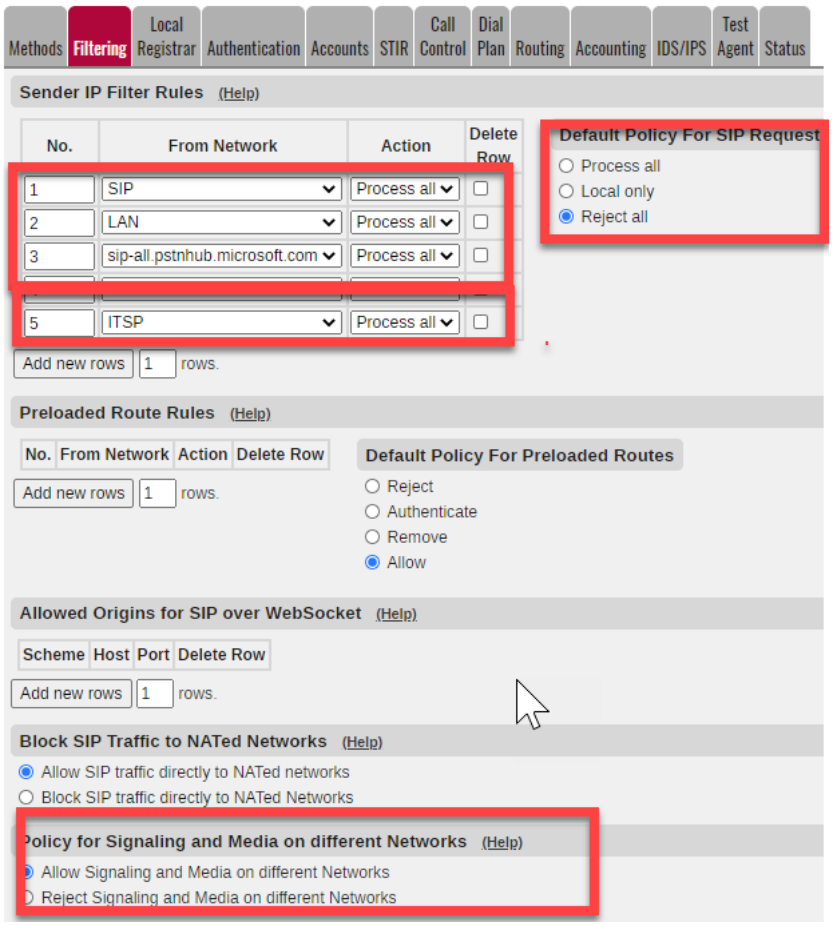
Always use Media Proxy.

Allow multiple sender IP addresses and ports.

Support Forked Media – Yes.

Always Relay Media – Yes.

Under SIP Traffic →Filtering



You might want to add some restrictions to process SIP traffic only from known sources. (Security)

Also, enable media and signaling coming from different networks.

2.1.10 Interoperability features

Leave default interoperability parameters, but ICE attributes must be stripped.

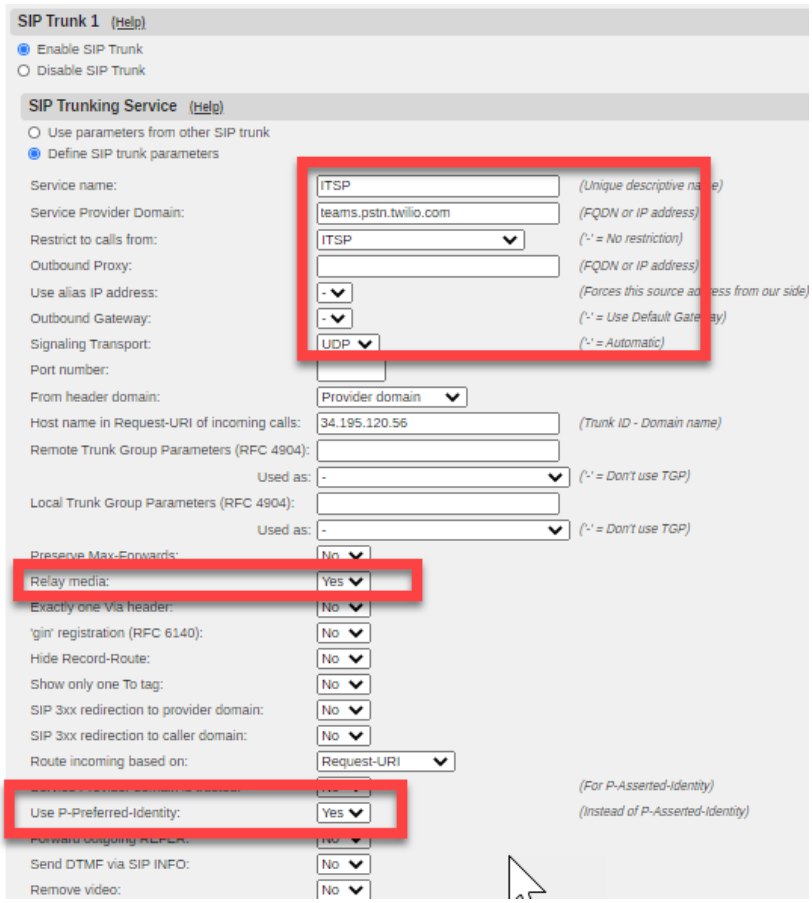
Under SIP Services → Interoperability:

2.1.11 ITSP SIP trunk Configuration

In most scenarios, specific configuration may vary from one ITSP to another. It will depend on specific requirements of the ITSP.

In our example the important thing is to pay attention to how the Inbound traffic will be managed and how outbound caller ID will be managed or manipulated.

In our example we are using Twilio ELASTIC Trunk Service.



Our ITSP uses UDP Transport

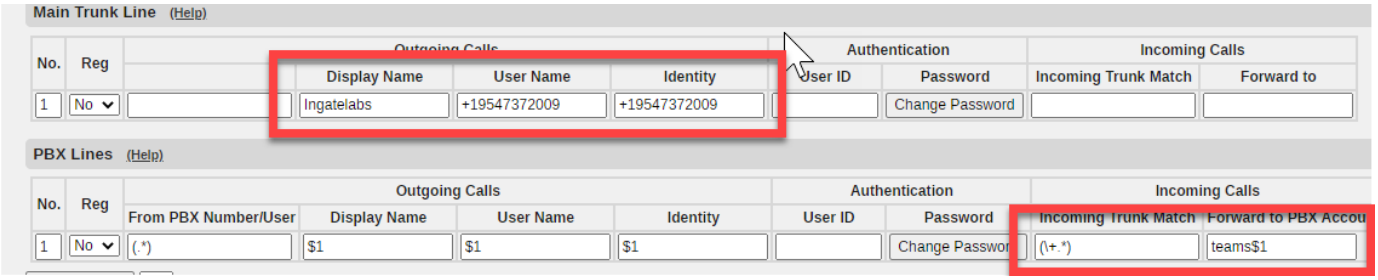
Enable **Media Relay**

Enable **P-Preferred-Identity** for caller ID

Remaining parameters stay at default values.

We assume the inbound R-URI user will be formatted using E.164, and is passed as such to Teams.

Any ingress traffic from the ITSP will be sent to the dial plan by routing the SIP requests to the local loop (127.0.0.1), adding a prefix "`teams`". This prefix allows the dial plan to match and properly route such requests to Teams.



As shown in the above picture, the default caller ID (**User Name**) and PAI (**Identity**) can be any E.164 number as needed, as well as the Display Name (**Display Name**). Otherwise (**From PBX Number/User**)

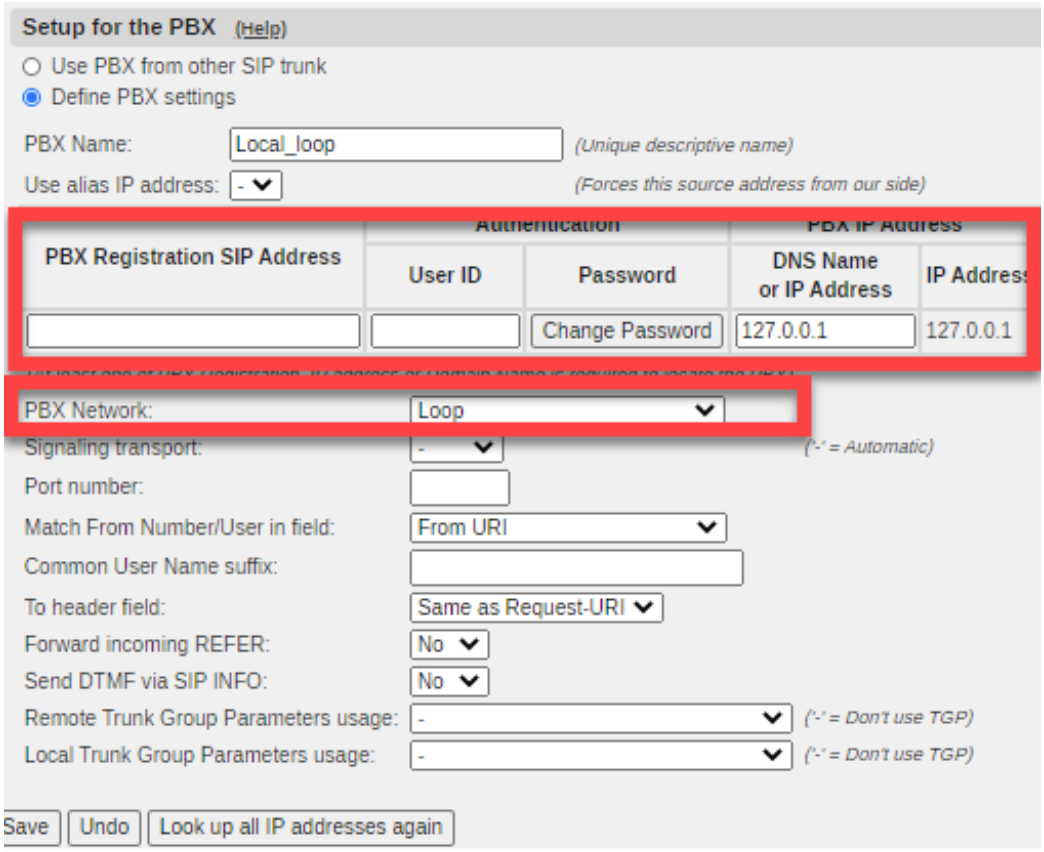
values coming from the Dial Plan can be manipulated as Shown in the Outgoing Calls Section of the PBX lines.

Minor changes may be needed if the carrier is not using E.164 format, but the R-URI user has country code, plus the 10-digit national number. In this case, the Incoming trunk match can be (.*) and the "Forward To" will add the "+" sign i.e. "`teams+$1`". If only certain DIDs will be routed to Teams, the Matching Trunk regular expression can be built to match the ones we need to route to Teams Cloud PBX.

Note: Use of Ingate's Generic Header Manipulation (GHM) provides here powerful and flexible ways to adjust according to your needs.

The PBX Section for the Trunk Group will point to the local loop (127.0.0.1) to be able to properly manipulate and process the call using the main dial plan (next section).

In our example the PBX has been named "`Local_loop`"



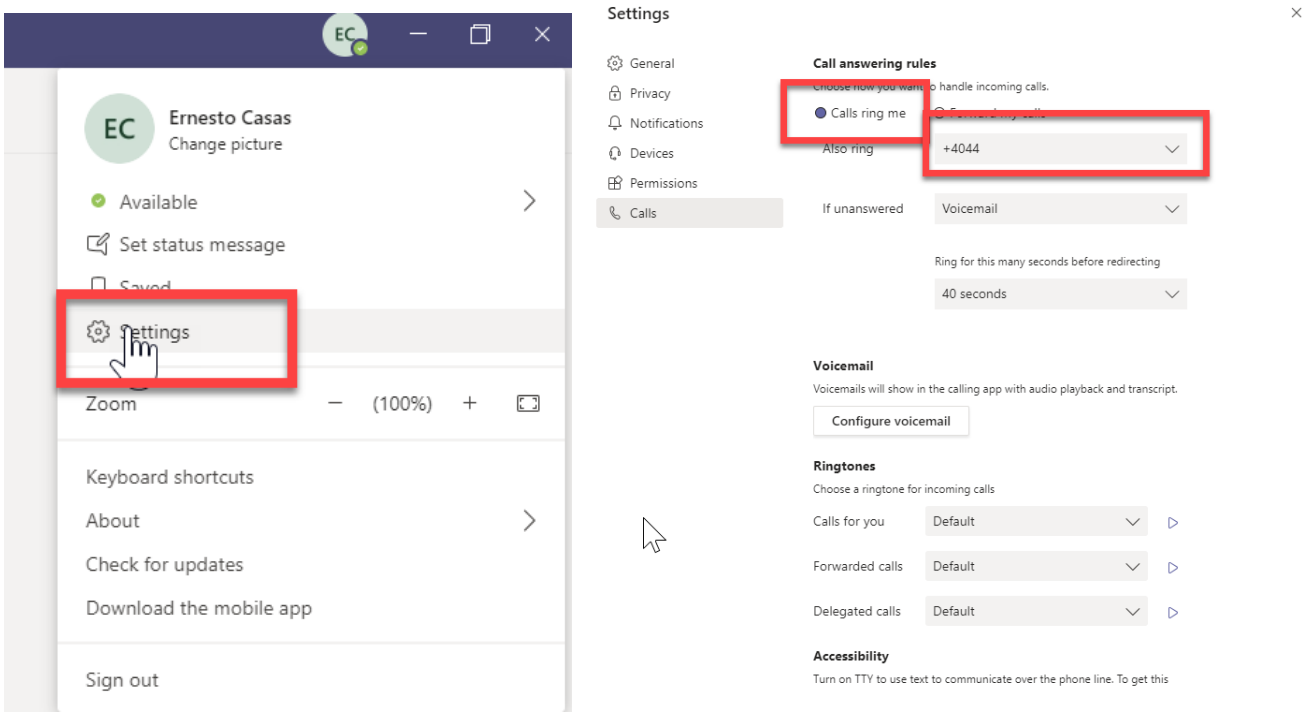
Additional Trunk groups can be used to route calls directly to the IPPBX for DIDs that do not have a configured destination in Teams.

2.1.12 Dial Plan

This section will show how calls from the ITSP are routed to Teams once the Trunk Group catches them, assigns a "`teams`" prefix and matches in the Dial Plan.

Our Dial Plan matches any call coming from Teams with R-URI user matching "+"sign and only 4 digits (+….), to route those calls to the PBX. This is done to enable Simultaneous ring for Teams users that also have a PBX extension and with its properly configured client.

Example of teams client setting with PBX simultaneous ring configuration:



In this example, Inbound (From PSTN) calls to the user DID ring in the teams client and simultaneously on extension 4044 in the PBX. Calls to the extension will be matched as a call coming from Teams to a `+<4digit>` destination and routed accordingly.

Dial Plan in detail:

1) Match From Header:
    a. Any SIP request coming from "Teams" network***. (From Teams)***
    b. Any SIP Request with from uri = sip:[^@]+microsoft.com and from "teams" ***network (Teams SIP OPTIONS)***
2) Matching Request-URI:
    a. R-URI matching expression: sip:\+?(....)@sbcteams.ingatelabs.com:5061 ***(To_PBX)***
    b. R-URI matching expression: sip:(\+1.....*)@sbcteams.ingatelabs.com:5061 ***(To_PSTN_USA)***

c. R-URI matching expression: sip:teams(.*)@127.0.0.1 ***(To_Teams)***. This will match routed inbound calls on the ITSP Trunk to be managed by this dial plan. (Local Loop)

3) Forward to: (Routes)

a. **ITSP:** Route to ITSP SIP Trunk ***(SIP Trunk 1:ITSP, Local_loop)***

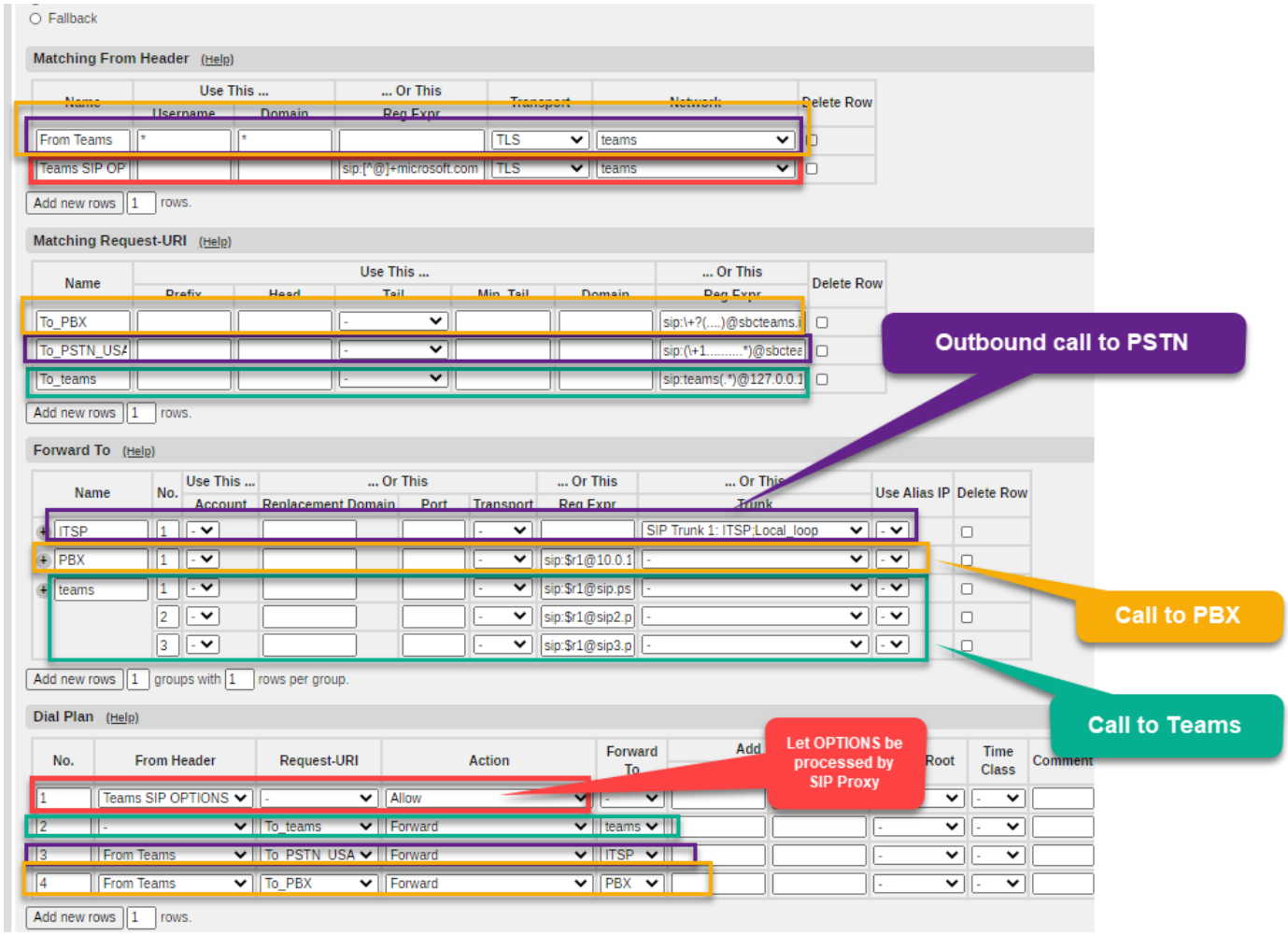
b. **PBX:** Route to PBX using destination captured in R-URI named $r1 ***(sip:$r1@10.0.1.114)***

c. **teams:** Route to Microsoft PSTN hubs (3) and adding

i. sip:$r1@sip.pstnhub.microsoft.com?To=%3csip%3a$r1%40$(to.host)%3e

ii. sip:$r1@sip2.pstnhub.microsoft.com?To=%3csip%3a$r1%40$(to.host)%3e

iii. sip:$r1@sip3.pstnhub.microsoft.com?To=%3csip%3a$r1%40$(to.host)%3e



4) Dial Plan (Rules are procesed in sequence based on the **No.** column):

a. If From header matches **Teams SIP Options**, just **allow** the request to be managed and answered by the proxy.

b. If Request-URI matches **To_teams**, forward the request to "**Teams**" Forwad To route.

c. If From Header matches "**From Teams**" and Request-URI matches "**To_PSTN_USA**" then forward the request to the ITSP Forward To route.

d. If From Header matches "**From Teams**" and Request-URI matches "**To_PBX**" then forward the request to the PBX Forward To route.

2.2 Additional considerations

The case shown here can be expanded to add more functionality, depending on your use case and final design.

For instance, it can be expanded to separate Inbound traffic to your PBX, or Teams, on a number of different criteria. E.g. determine the call destination based on DID. You can even use call control (REST API/cURL features included in SIParator firmware) to perform lookups to an external application for the location of the final DID destination. This application could, for instance, query the Active Directory.

Inbound discrimination to Teams or PBX can also easily implement an additional Trunk Group for PBX DIDs and use the appropriate matching regular expressions on the Incoming Trunk Match field.

This worked example does not include routing calls from the PBX to Teams clients. It can be added very easily. In a new document, we will also add a special use case, using a single SBC with Microsoft Office Multi-tenant, i.e. multiple domains.

Should you need an assessment of your specific case, you are welcome to contact our sales team and they will set up a conference with our experts to review and discuss your case.

3 Troubleshooting

When configuring your environment, it is possible you will encounter problems. We outline here a few symptoms which will help to get you on track.

3.1 You lack mTLS

Once you have configured `SIP OPTIONS` pings to the MS Teams infra, check the SIP logs on the Ingate. If you see messages like these:

```
2020-10-01 15:48:13.135                    >>> Debug: sipfw: TCP handshake for TLS connection 2890 OK.
2020-10-01 15:48:13.197                    >>> Debug: sipfw: TLS handshake for connection 2890 OK.
2020-10-01 15:48:13.198                    >>> Info: sipfw: send sf (0x56295dca18c0) to 52.114.75.24:5061: OPTIONS sip:sip.pstnhub.microsoft.com;transport=tls SIP/2.0
2020-10-01 15:48:13.199
>>> Info: sipfw:      send sf (0x56295dca18c0) to 52.114.75.24:5061 via 193.180.23.82:23031 TLS connection 2890:

                     OPTIONS sip:sip.pstnhub.microsoft.com;transport=tls SIP/2.0
                     Via: SIP/2.0/TLS 193.180.23.82:5061;branch=z9hG4bK439c7a7f77e5da5a6e52d53863f32b57
                     From: <sip:sip.pstnhub.microsoft.com;transport=tls>;tag=7d01077a
                     To: <sip:sip.pstnhub.microsoft.com;transport=tls>
                     Call-ID: 38947245-111c2acd549-7e7a851d@sipgt-1ccdb45d
                     CSeq: 855114286 OPTIONS
                     User-Agent: Franken/1
                     Max-Forwards: 0
                     Content-Length: 0

2020-10-01 15:48:13.200                    >>> Notice: sipfw: 52.114.75.24:5061 (connection 2890, socket 41): SSL_read().: protocol-violating EOF seen
2020-10-01 15:48:13.200                    >>> Debug: sipfw: TLS connection 2890 (0x56295dc8f560) closed (socket 41).
```

They are a very strong indicator that you have only TLS configured, and not mTLS (Mutual TLS).

In summary – the message "`SSL_read().: protocol-violating EOF seen`" means that the MS Teams end disconnected, because it could not verify the signing CA of your device certificate.

Resolution: Ensure that the certificate (chain) uploaded to the private (device) certificate slot also has the (intermediate) signing CA included. The CA for the peer certificate must also be uploaded in the TLS CA Certificates table.

Review the steps here: **Configure SIP TLS with the certificates**

Once resolved, you will start to receive replies to `SIP OPTIONS` pings, and healthy logs should look similar to this (whether 200 OK or 403 is not important, but that you should be able to form a TLS connection):

```
2020-10-01 15:54:46.172
>>> Info: sipfw:             send sf (0x560c731583c0) to 52.114.7.24:5061 via 193.180.23.2:15765 TLS connection
246926:

               OPTIONS sip:sip.pstnhub.microsoft.com;transport=tls SIP/2.0
               Via: SIP/2.0/TLS 193.180.23.2:5061;branch=z9hG4bK9aff4c759e84ad441df0221e9575dd32
               From: <sip:xx.company.com>;tag=7de8e4ff
               To: <sip:sip.pstnhub.microsoft.com;transport=tls>
               Call-ID: 609754fa-2496d431aca-2ed7b29e@zyzzyx-49c52a68
               CSeq: 1334584138 OPTIONS
               User-Agent: Ingate
               Max-Forwards: 0
               Contact: <sip:xx.company.com:5061;transport=tls>
               Content-Length: 0
2020-10-01 15:54:46.388      >>> Info: sipfw: Destination 52.114.7.24:5061 now up
2020-10-01 15:54:46.388      >>> Debug: sipfw: Recv 548 bytes from 52.114.7.24, connection 246926
2020-10-01 15:54:46.388
>>> Info: sipfw:             recv from 52.114.7.24:5061 via 193.180.23.2:15765 TLS connection 246926:

               SIP/2.0 403 Forbidden
               FROM: <sip:xx.company.com>;tag=7de8e4ff
               TO: <sip:sip.pstnhub.microsoft.com;transport=tls>
               CSEQ: 1334584138 OPTIONS
               CALL-ID: 609754fa-2496d431aca-2ed7b29e@sipgt-49c52a68
               VIA: SIP/2.0/TLS 193.180.23.2:5061;branch=z9hG4bK9aff4c759e84ad441df0221e9575dd32
               REASON: Q.850;cause=63;text="c2d83042-847e-4c88-8620-23fdb2e89eac;Fail to fetch trunk data for
trunkFqdn: xx.company.com. Status code: NotFound"
               CONTENT-LENGTH: 0
               ALLOW: INVITE,ACK,OPTIONS,CANCEL,BYE,NOTIFY
               SERVER: Microsoft.PSTNHub.SIPProxy v.2020.9.21.1 i.ASEA.6
```

4 Additional help or support

If you have questions, suggestions and any other concern feel free to contact Educronix LLC

Web: www.educronix.com
Email: support@educronix.com
Toll-Free: +1 855 866 8854
Ph: +1 954 866 8884

We also provide consulting services as well as remote hands troubleshooting and configuration.