Setting up Ingate's

SIParator® / Firewall®

For

MiVoice Connect

&

Using Tie Lines

For Ingate SIParators using software release 6.3.2 or later

Revision 1.0

August 2021

Table of Contents

1 Minimum Requirements

1.1 SIParator Version

This document applies to :

- SIParator/Firewall Version 6.3.2 or later.
- All Ingate Models, physical and virtual or Cloud (i.e. VMWare, Hyper-V, KVM, VirtualBox, 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 Call2Teams. It might depend on the number of simulatenous calls between MiVC and Teams Clients

Additional Trunk Licenses with shared or additional CCS to route traffic to an IP PBX if necessary. (ask sales@ingate.com if any advise is needed)

SIP registrar Users (SRU), equivalent to the number of Teams clients that will be interchanging sessions with MiVC. For instance, if you have 10 Teams users and all of them will need to be reached from any MiVC extension, you'll need 10 SRU.

For additional license needs or questions, connect with your Ingate representative or email to sales@ingate.com.

1.3 Call2Teams Account.

You'll need to have a Call2Teams account provisioned for as many Teams Users will participate in this interconnection. For more details on how to Provision an account via a C2T Partner:

For USA: https://www.call2teams.com/find/partner/?_sft_location=usa&_sft_specialism=mitel

For Canada: https://www.call2teams.com/find/partner/?_sft_location=canada&_sft_specialism=mitel

For Europe: https://www.call2teams.com/find/partner/?_sft_location=europe&_sft_specialism=mitel

… and many more.

1.4 FQDN/Public IP for the SBC

A specific Public IP address and an FQDN is needed for the SBC to be reached from C2T infrastructure

1.5 Public Trusted certificate.

An SSL Certificate, properly signed by a Trusted CA will be needed for the SBC if you are planning to use TLS between the SBC and C2T infrastructure.

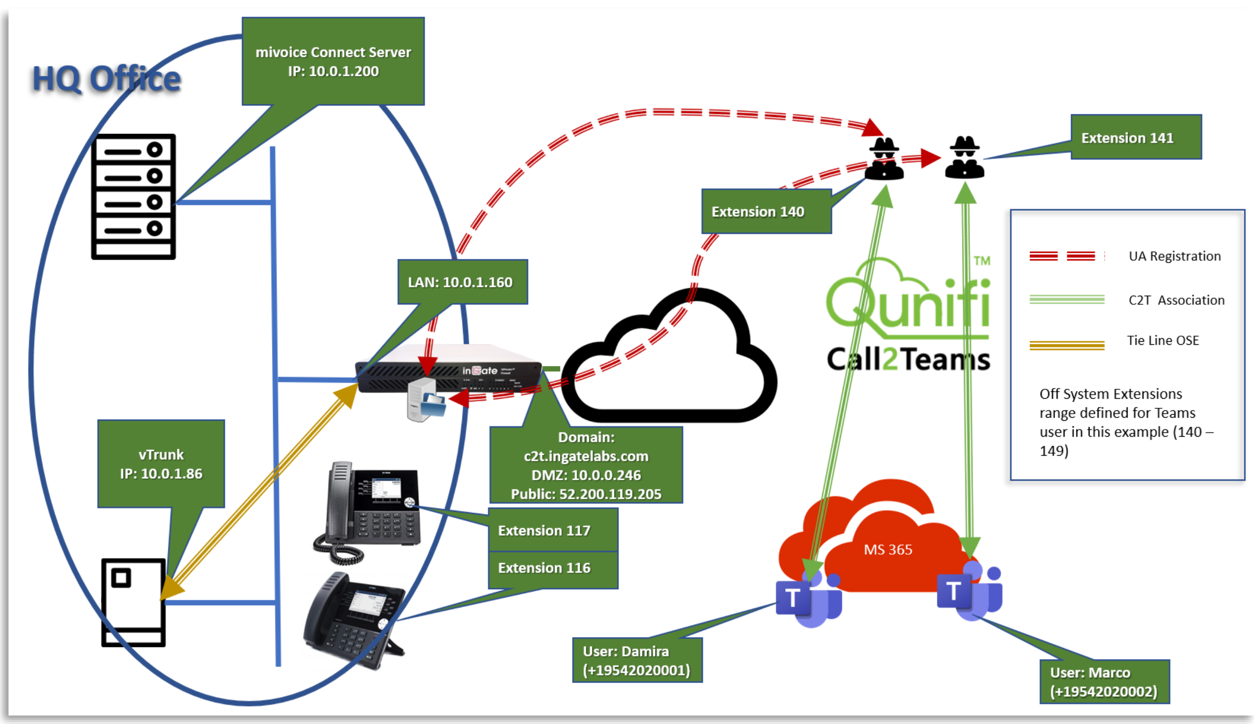
1.6 MS Teams Requirements.

We are assuming you have already accomplished all requirements needed in the MS Teams and MS 365 side to implement Call2Teams.

2 SIParator configuration

The next subsections explain in detail how to configure your SIParator SBC in typical use case scenarios. We are using a real Lab deployment used to proof concept this case

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). In our case such IP will be 52.200.119.205 and the FQDN associated will be c2t.ingatelabs.com

In case you are planning to use TLS between the SBC and Call2Teams, a Public Certificate, issued by trusted CA. This certificate will be installed in the SBC as a Server Private Certificate.

Proper Root certificates will be needed installed in the CA certificate section in the SBC. To be able to support a broad set of Trusted Certification Authorities we suggest installing this bundle: https://curl.se/docs/caextract.html

2.1.2 SBC Domain / FQDN

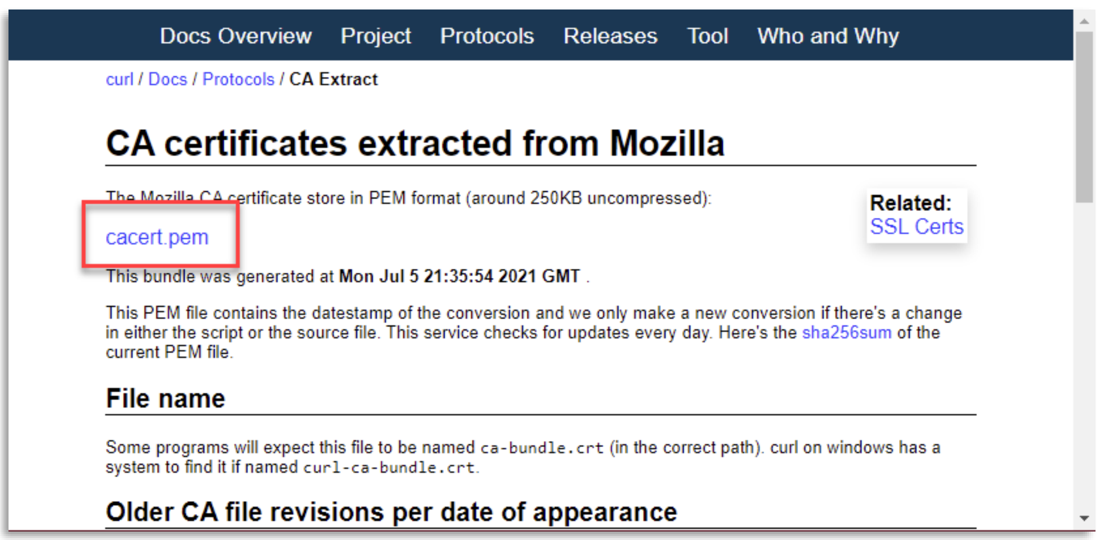
The SBC Domain will be used for C2T registration in the SBC. The SBC will have configured and enabled registration for every C2T user and will need to have preloaded all the credential for such users.

In our Lab example we are installing 2 user registrations associated respectively to 2 Teams Users, like this:

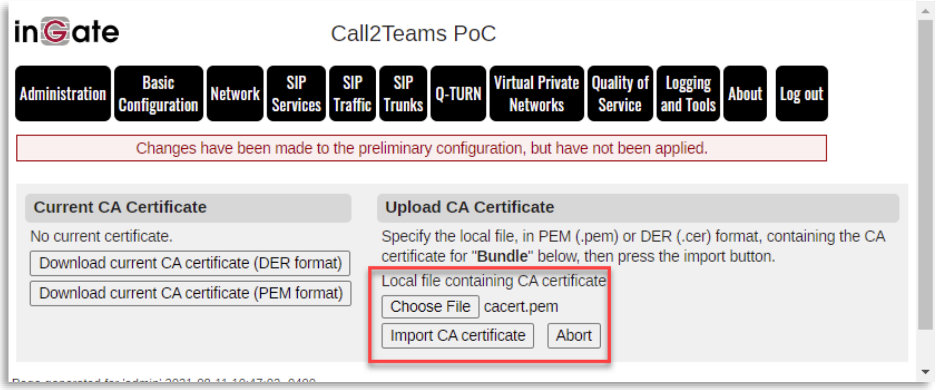
Teams User	Teams DID	SIP User for C2T
Ernesto Casas (ersnesto@ingatelabs.com)	+19547372001	140
Marco Casas (marco@ingatelabs.com)	+19547372023	141

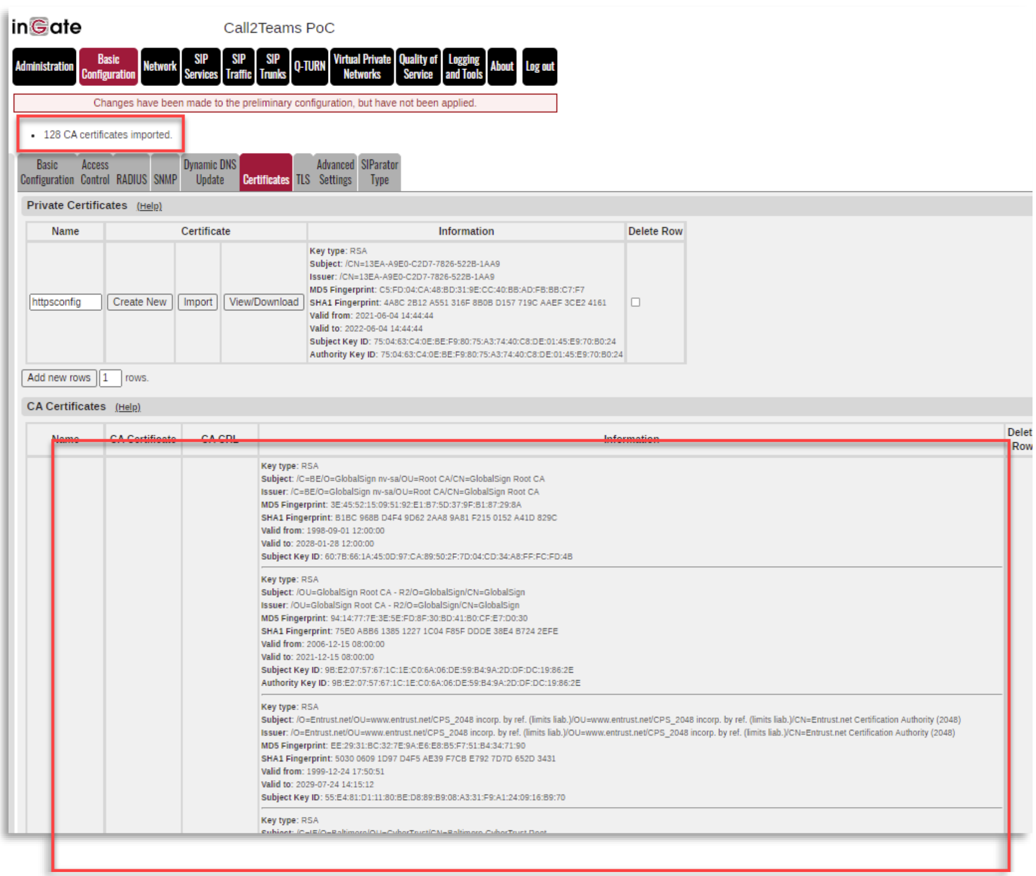
2.1.3 Deploy CA Certificates and Configure SIParator TLS Certificate (If needed).

First we'll need to load Certification CA roots certificates from suggested bundle. Download pem certificate:



Import pem certificates bundle into SIParator CA Certificates:

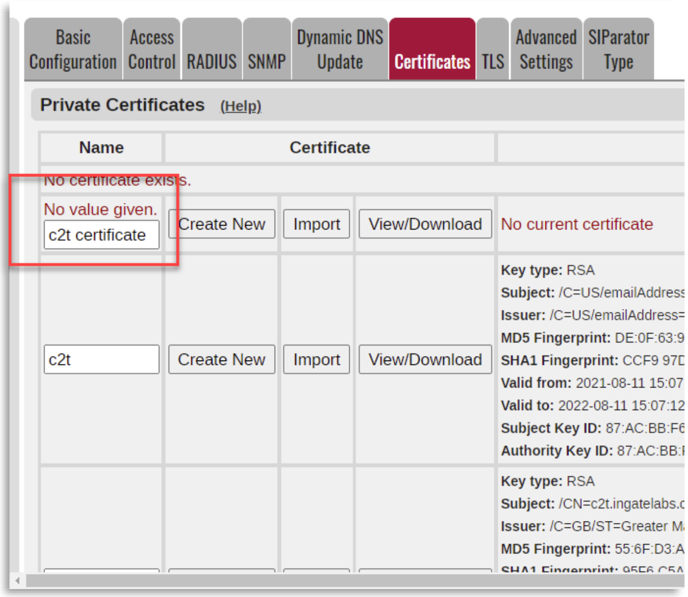




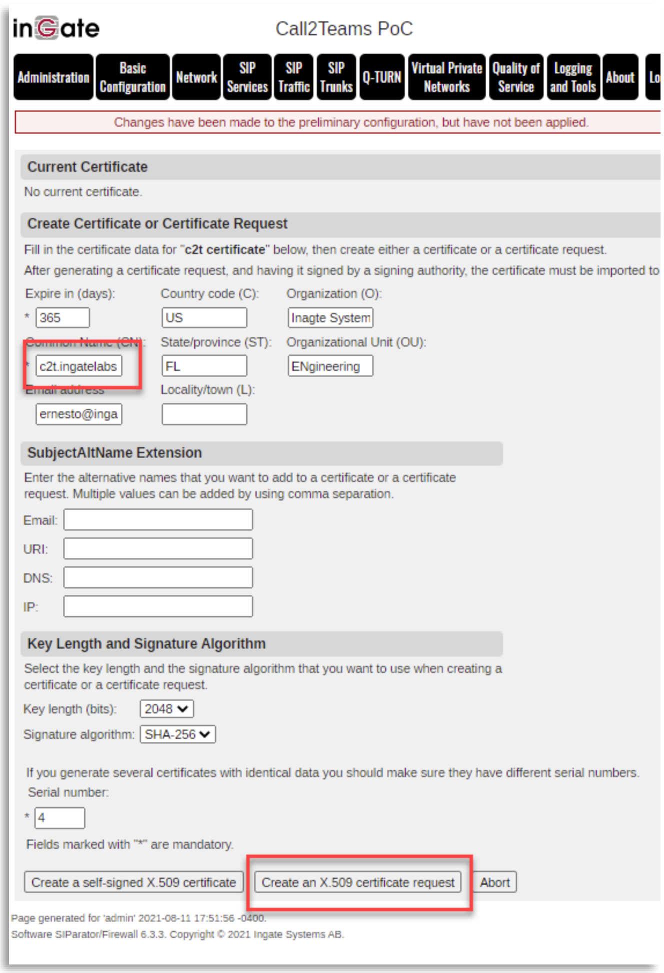
In our example we will add Signed Certificates from Sectigo obtained via Namecheap.com. In order to obtain the signed certificate, you need to create a CSR (Certificate Signature Request) using the SIParator:

In Basic Configuration → Certificates:

Add a new row on Private Certificates:



Assign a name and click on "Create New"

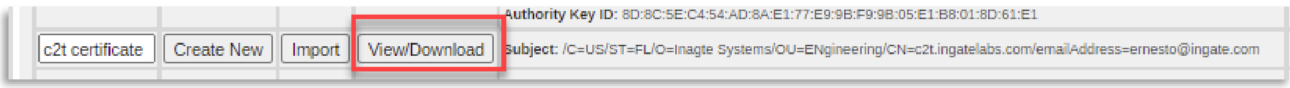


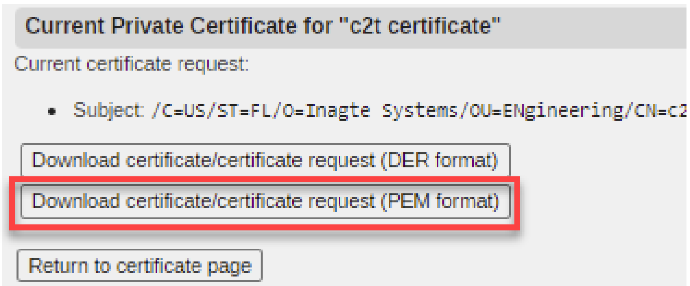
Fill in all needed information and make sure the Common Name (CN) matched the Domain you are planning to use. In our example "c2t.ingatelabs.com".

Then click on "Create an X.509 certificate request"

At this point you should be able to download the CSR to be used and provided to the Certification Authority of your selection for further signature.

Click on "View/Download" of the new certificate request





PEM would be the most common format accepted by any CA.

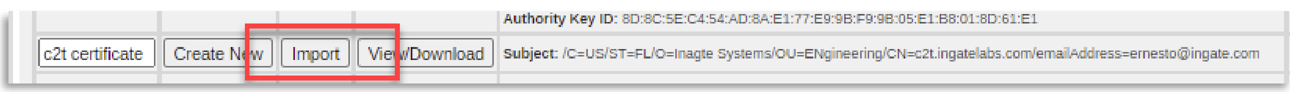
Click on download certificate/certificate request (PEM format)

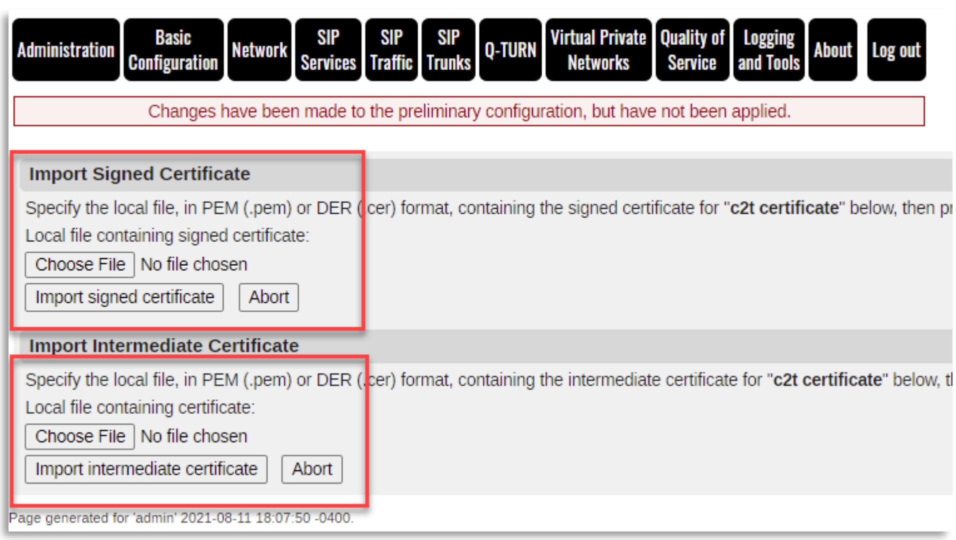
Use the file to be submitted to the CA for further signature.

Once you get the response from the Signing Authority, you will receive the signed certificate and in some cases a bundle of additional (Intermediate) certificates that might be needed.

To load the signed certificate:

Go to the Certificate and click on "Import":





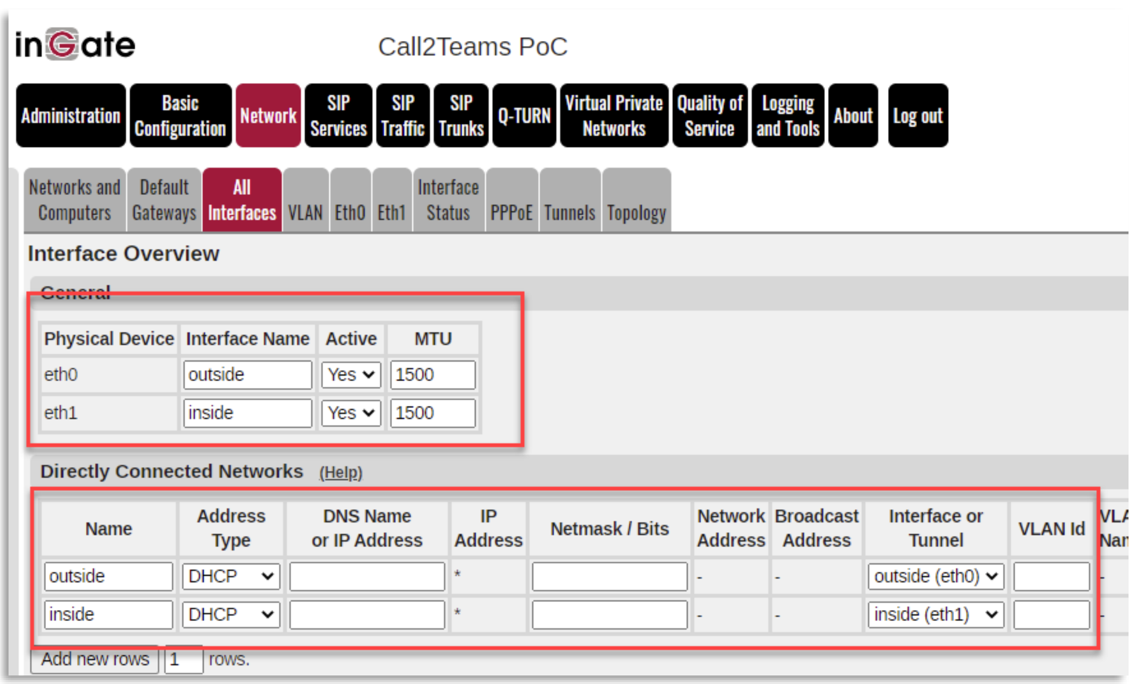
First "Choose File and Import Signed Certificate" and once it is loaded go again to the same screen to chose Any intermediates bundle provided by the CA and Import them (If needed).

At this point you are prepared to deploy TLS to secure communications between Call2Teams infrastructure and your SIParator.

2.1.4 SIParator Network configuration

In this example we will show required Network configuration in the DMZ topology and specific for this use case. This might be a little different if you are deployin C2T integration with other existing services in your SIParator. Our Support team can always provide you additional guidance if needed for your specific scenario (just open a ticket with support@ingate.com)

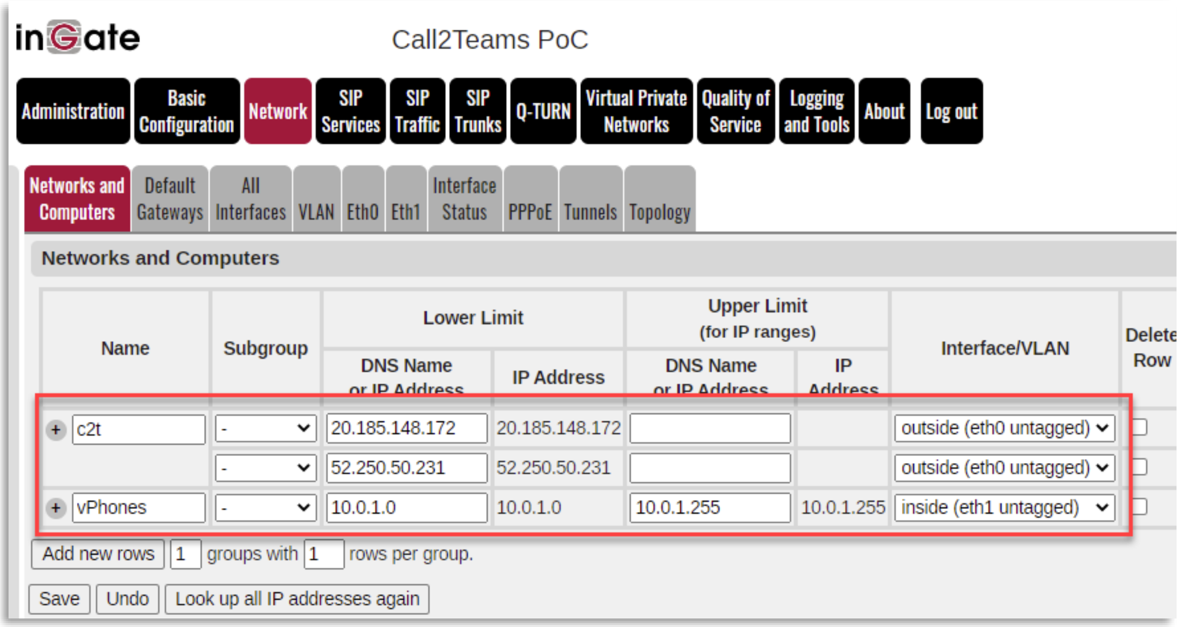
Here, eth0 will be in the DMZ (outside) and eth1 will be on the LAN (inside). In our Lab environment all preassigned IP's are managed by DHCP Service, so configuration will look like:



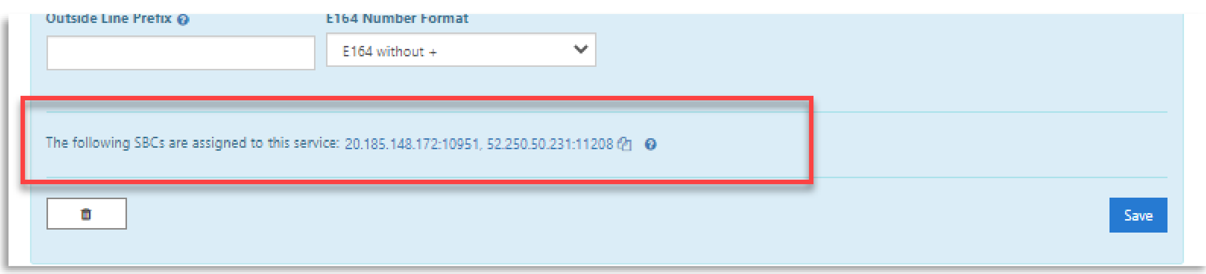
You might need to add any static routes depending on your internal network topology.

We will create a set of network names to facilitate configuration. You might have already some names defined, so you just need to add the ones that haven't been considered yet.

Under Networks → Networks and Computers:



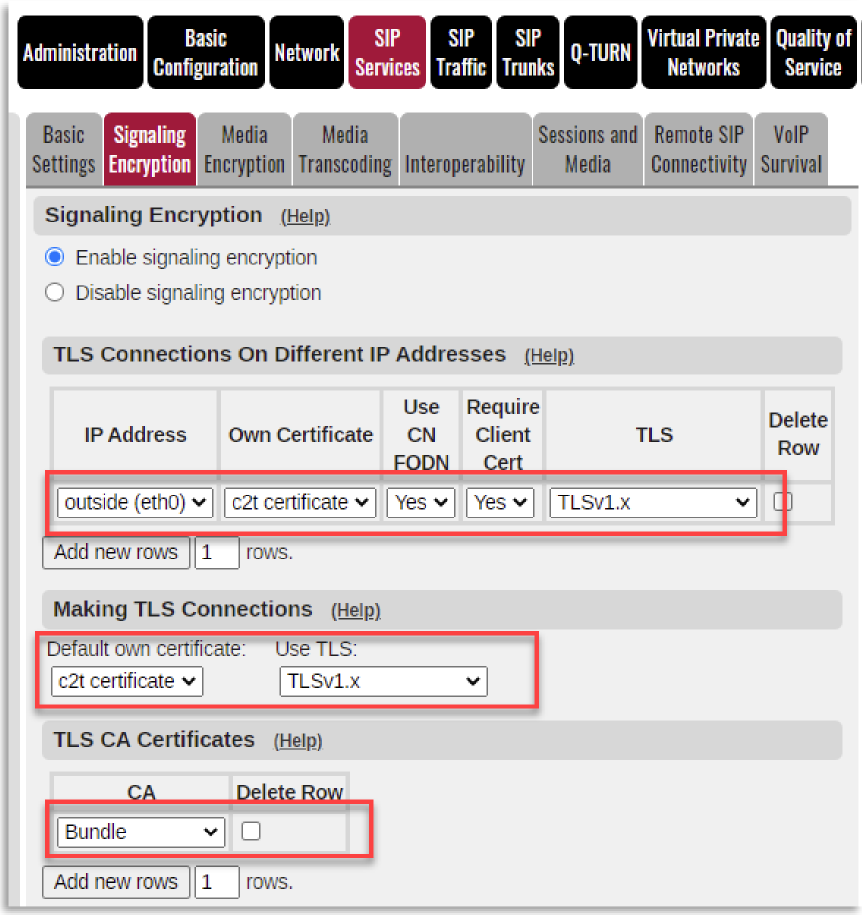
- **c2t**: IP addresses pre-assigned and allocated by Call2Teams and can be obtaniend from Call2Teams administration portal (https://admin.call2teams.com/portal/) , under Services section → PBX at the bottom:



- vPhones: IP addresses of ranges where the Switch to be used for Tie Trunk is located. In our example to make it flexible and broad enough we are including all IP range for the Inside LAN.

2.1.4.1 Configure SIP TLS with the certificates (If needed)

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)

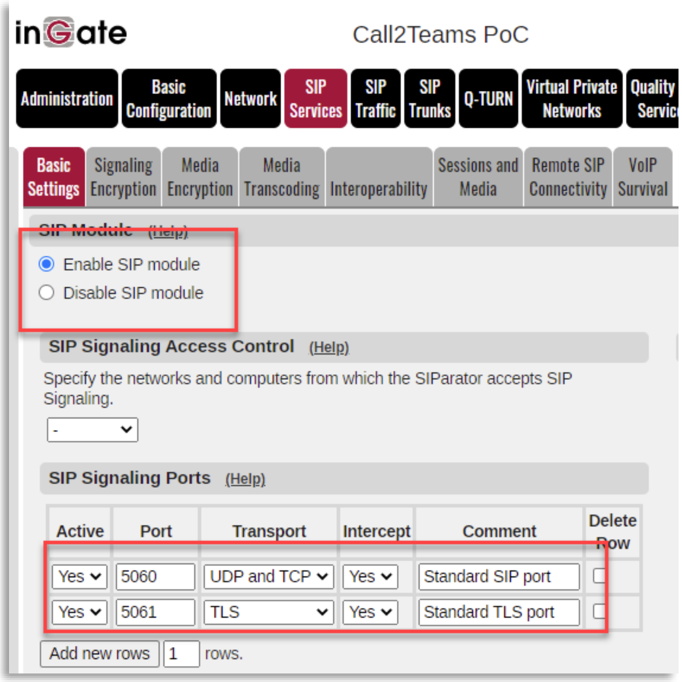
Select TLSv1.x in the TLS column.

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

Under "**TLS CA Certificates**" Select the bundle you loaded in the CA Certificates at the beginning of this document.

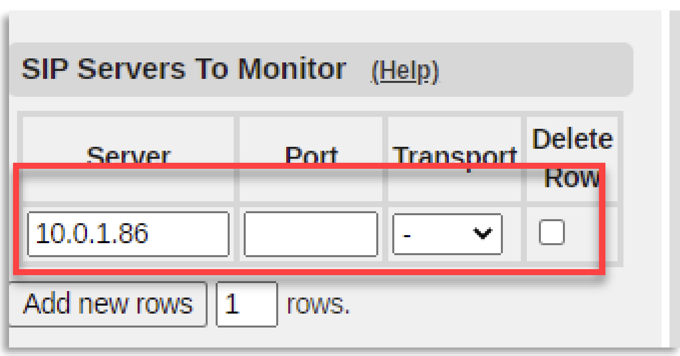
2.1.5 Configure SIP Signaling

In this section, enable UDP ports to be used with your IPPBX as well as the ITSP, and TLS to be used with Call2Teams if you decided to do so.



Enable the SIP module

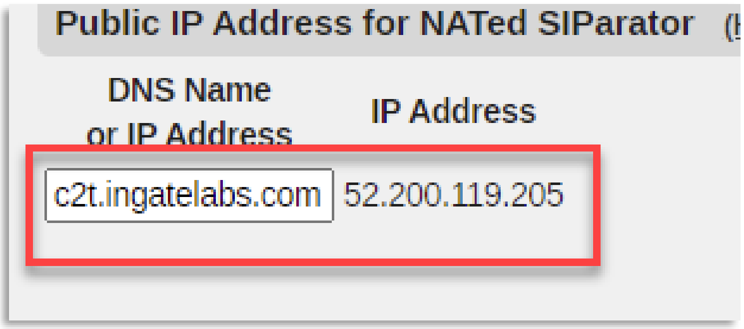
Under **SIP signaling ports**, make active port 5060 for TCP and UDP, as well as 5061 for TLS. In both cases select Intercept "Yes"



Add to **SIP Monitor** FQDNs for the Switch you are going to use for the Tie Trunk between SIParator and MiVC platform.

Add any other SIP point that you consider should be monitored.

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



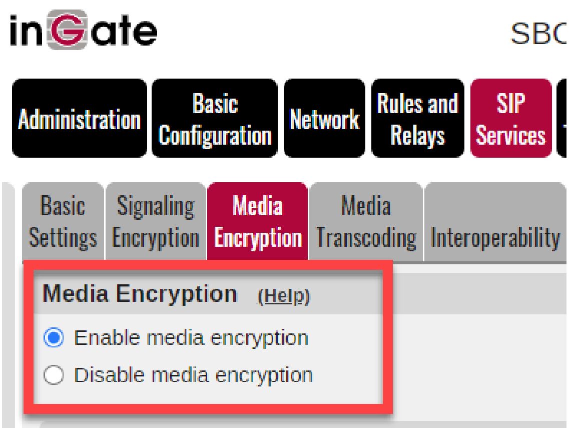
In this use-case scenario, the SIParator external interface is connected to a private DMZ, we add the external public IP address, which corresponds to the SBC FQDN. In our case:

c2t.ingatelabs.com.

Enter the FQDN or the Public IP.

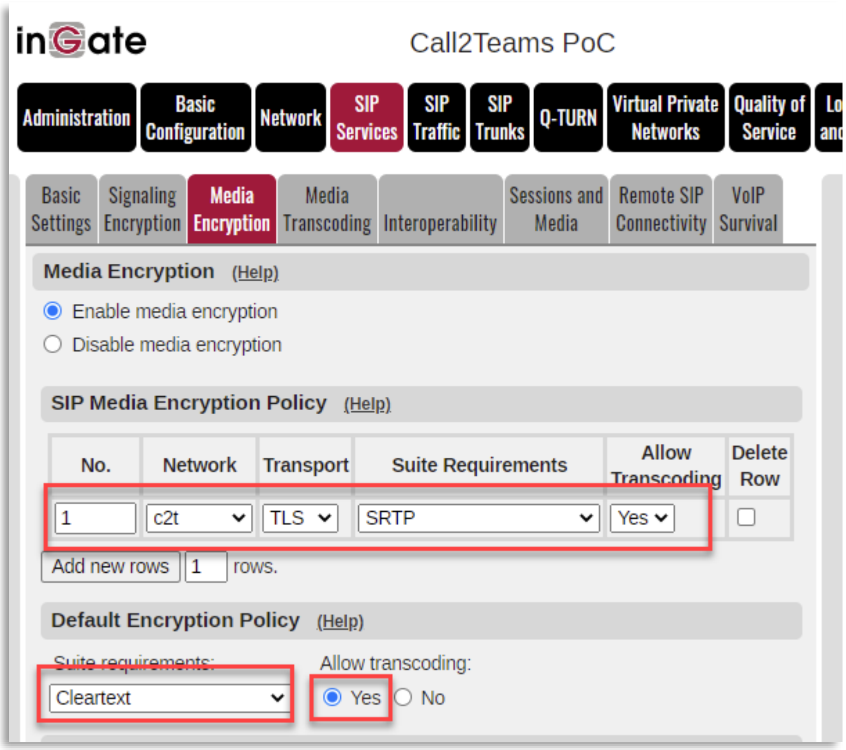
2.1.6 Configure Media Encryption

First, under SIP Services → Media Encryption:



Enable **Media Encryption**

Assuming Media Encryption happens only between the SBC and Call2Teams, define it like this:

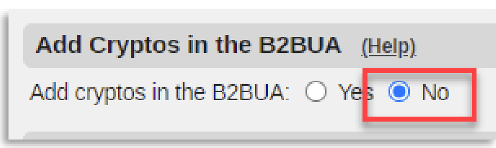


Add a **Media Encryption Policy** to apply the SRTP suite to c2t Network when TLS transport is used

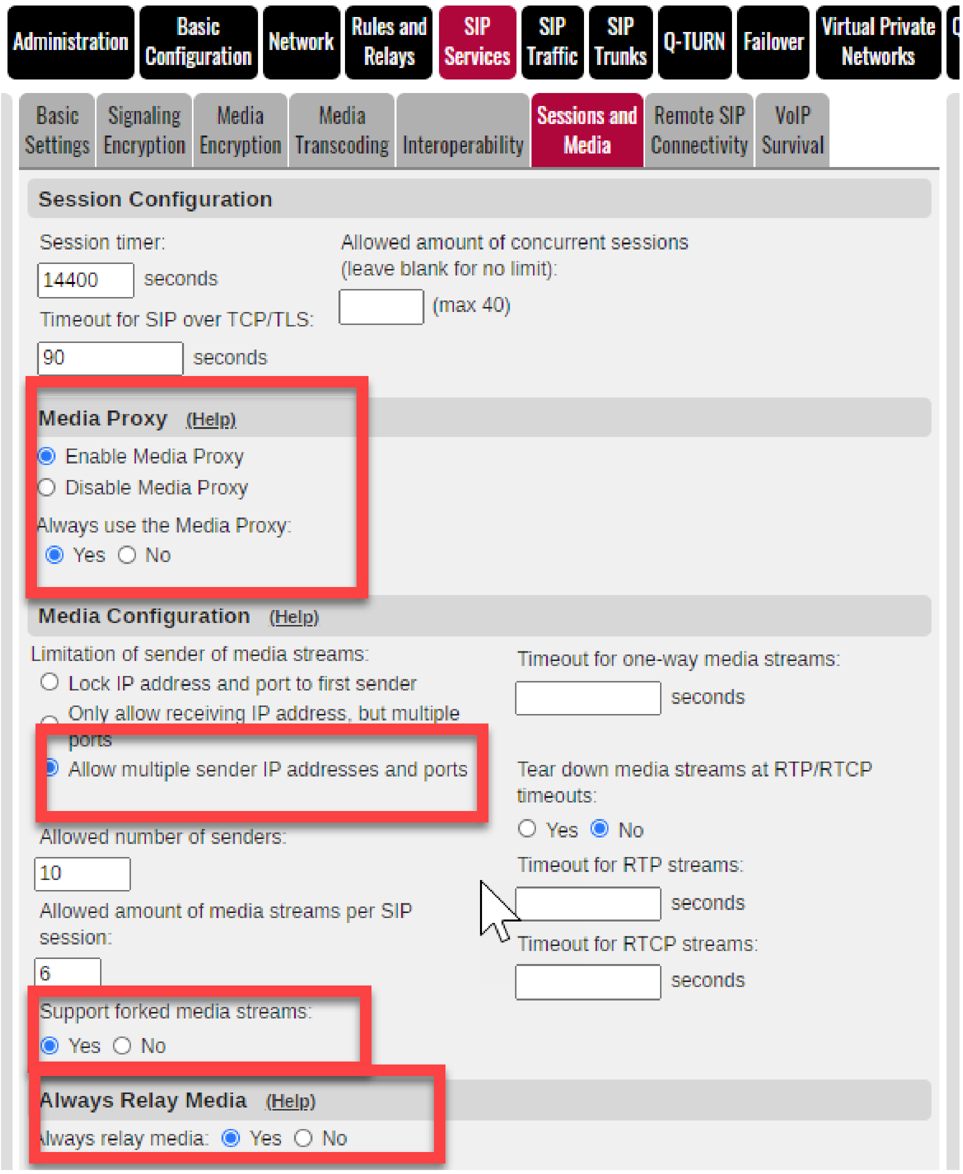
Allow **transcoding**

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

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



2.1.7 Other Media related configuration



Enable Media Proxy.

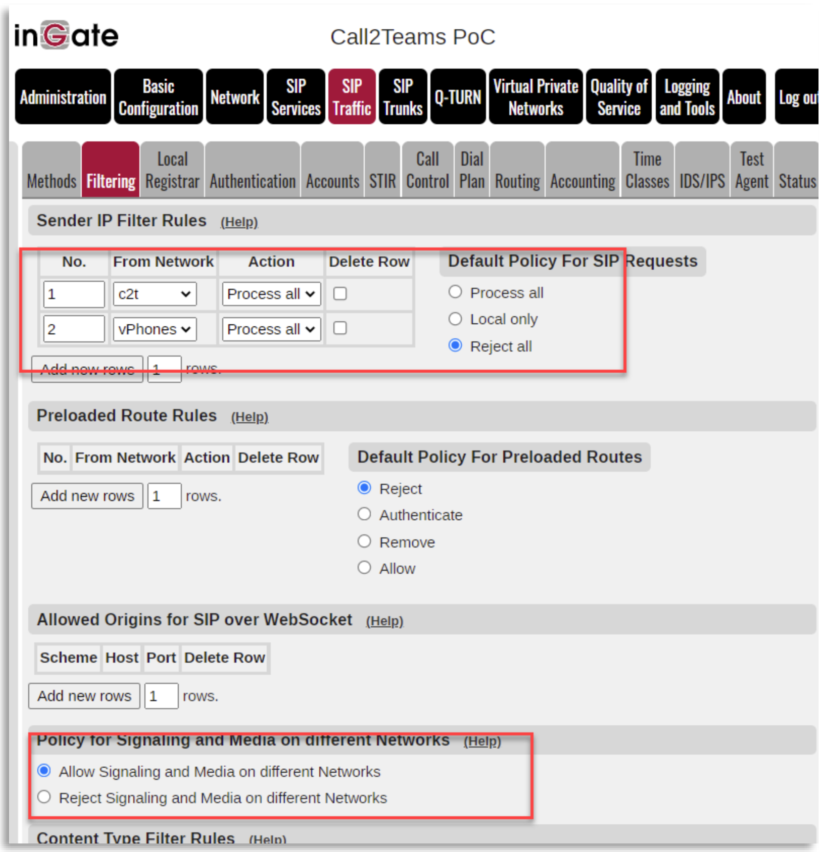
Always use Media Proxy.

Allow multiple sender IP addresses and ports.

Support Forked Media – Yes.

Always Relay Media – Yes.

Under SIP Traffic →Filtering

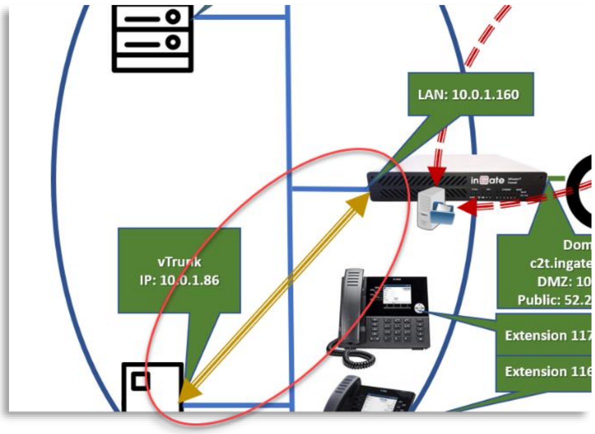


You might want to add some restrictions to process SIP traffic only from known sources. (Security)

Also, enable media and signaling coming from different networks.

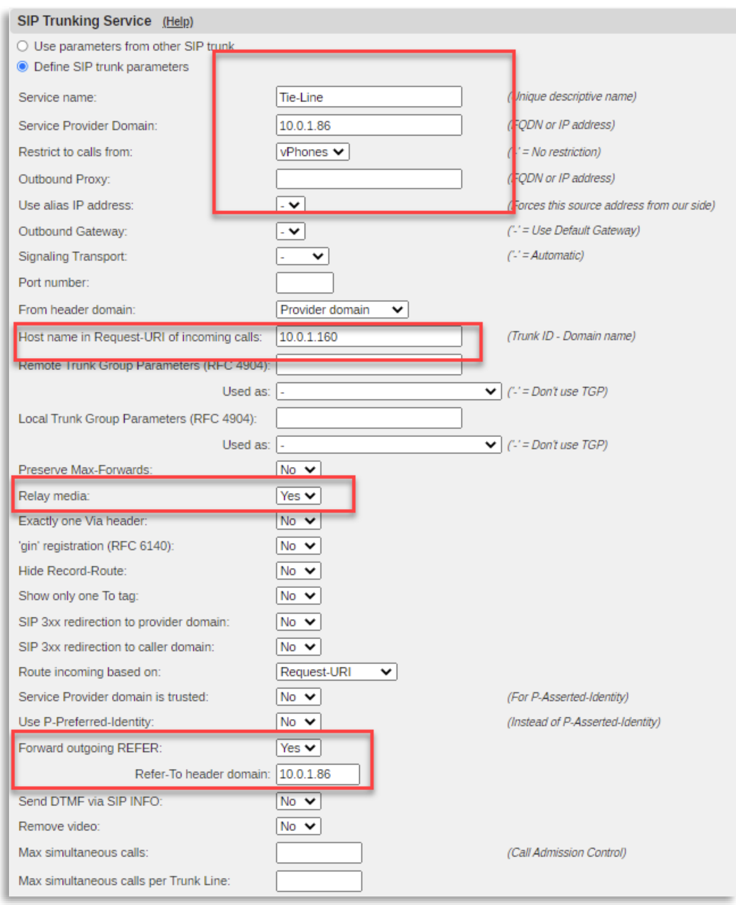
2.1.8 Tie Trunk Configuration

Going back to our original layout, we will build a Tie Trunk between MiVC and SIParator as shown in yellow line here:



Tie Line on the SIParator side will be a Trunk Group pointing to MiVC Switch where the trunk is going to be provisioned (via MiVC Director)

The main difference with a traditional Trunk Group is the that the (usually) PBX side will be pointing to the domain managed by the SIParator (in our case c2t.ingatelabs.com), so the SIParator will automatically reach the c2t virtual endpoints as they are already registered in.



Lets call this trunk **Tie-Line**

It will be pointing to the Trunk Switch selected in MiVC (**10.0.1.86** in our example)

Use **UDP** Transport

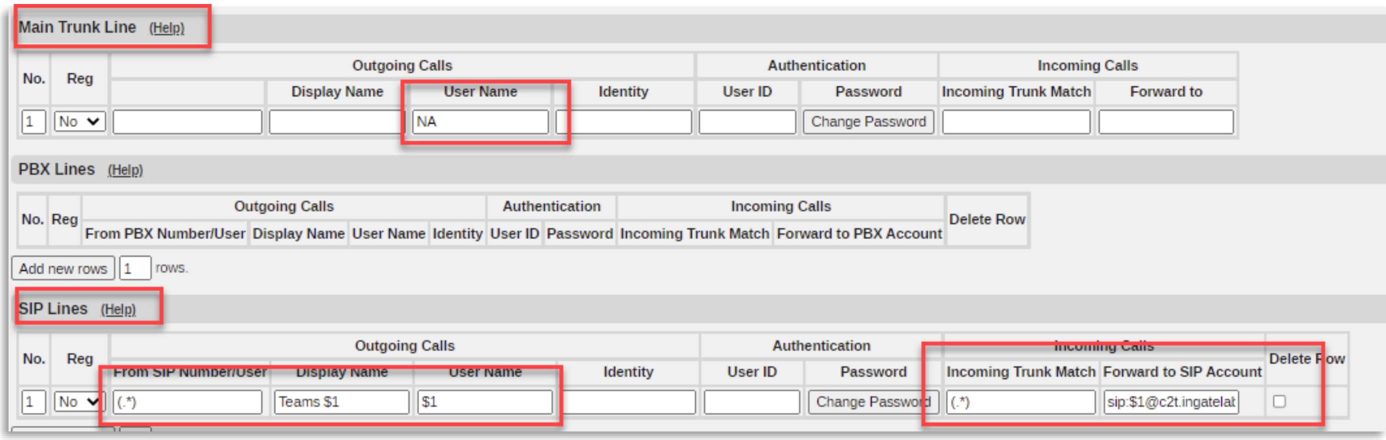
We will filter inbound calls identifying r-URI matching the SIParator inside IP (**10.0.1.160**)

Restrict calls to **vPhones** Network we defined previously (Any IP on our LAN side

Enable **Media Relay**

We will allow **REFER forwarding** to the Trunk Switch and replace host with the Switch IP address (**10.0.1.86**)

Any ingress traffic from the Trunk Switch will be sent to the dial plan by routing the SIP requests to the domain using SIP Lines.. Call will be routed to the user sent by the Switch in the Domain managed by the SIParator (**sip:$1@c2t.ingatelabs.com**)

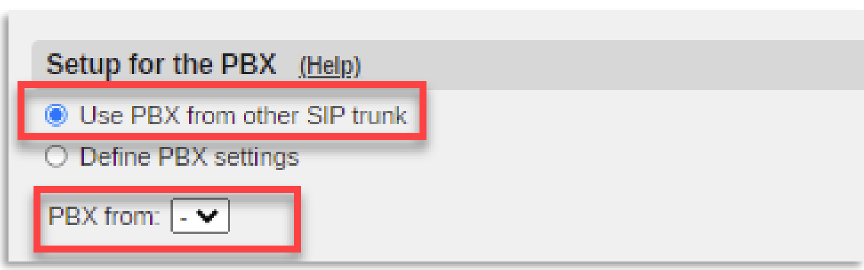


We will make c2t.ingatelabs.com domain a locally managed domain, when in create the local registrar credentials for all teams users later in this document.

As shown in the above picture, the default caller ID (**User Name**) and PAI (**Identity**) are not used number, as well as the Display Name (**Display Name**), just need any value (NA) in the User Name. In the Outgoing call section inside SIP Lines we will capture Frem header information coming from Call2Teams (**From PBX Number/User**) values via the Dial Plan. It can be manipulated as Shown in the Outgoing Calls Section of the SIP lines. (i.e. we are adding "Teams" to the caller name.

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

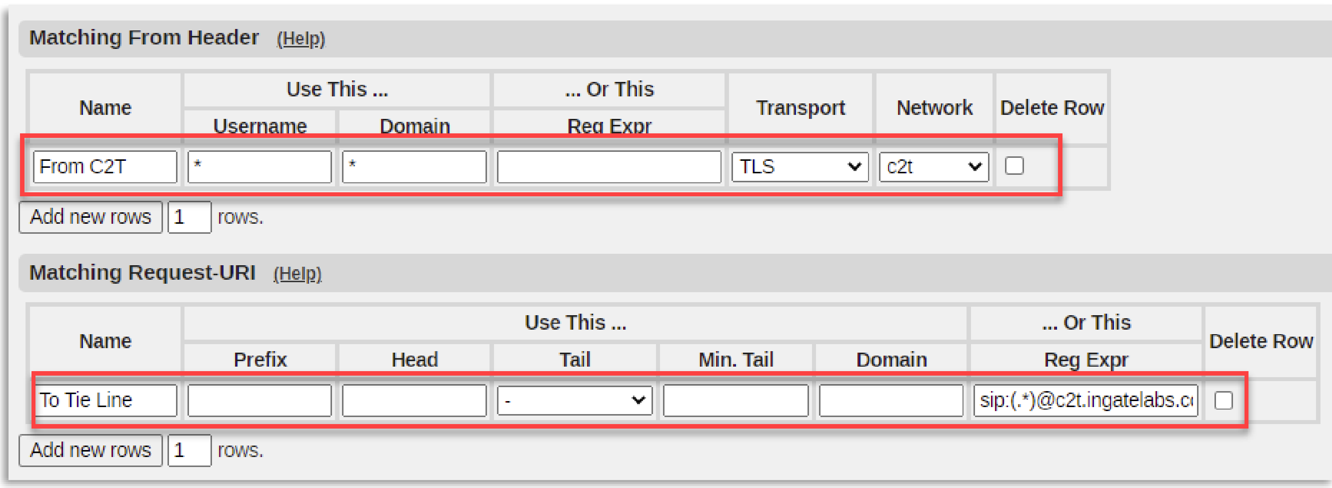
In The PBX Section we wont add anything as there is not a real PBX on the other end of the Tie-Lie, but the virtual users registered from Call2Teams in the SIParator registrar.



2.1.9 Dial Plan

This section will show how calls from the Trunk Switch (10.0.1.86) are routed to Call2Teams once the Trunk Group catches them, and because is routed to a locally managed domain will reach the local registered extension. As the SIParator is actually acting as a SIP Proxy and Registrar/Location Sever, ir will immediately rote the calls to the appropriate user in Call2Teams..

First we will match all requests originated from C2T network and having as the request-uri the pattern sip:(.*)@c2t.ingatelabs.com



Matching From Header (Help)

Name	Use This ...		... Or This	Transport	Network	Delete Row
	Username	Domain	Reg Expr			
From C2T	*	*		TLS	c2t	☐

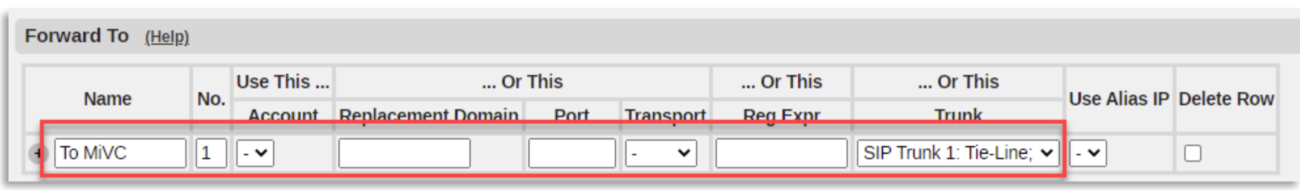
Add new rows 1 rows.

Matching Request-URI (Help)

Name	Use This ...					... Or This	Delete Row
	Prefix	Head	Tail	Min. Tail	Domain	Reg Expr	
To Tie Line			-			sip:(.*)@c2t.ingatelabs.c	☐

Add new rows 1 rows.

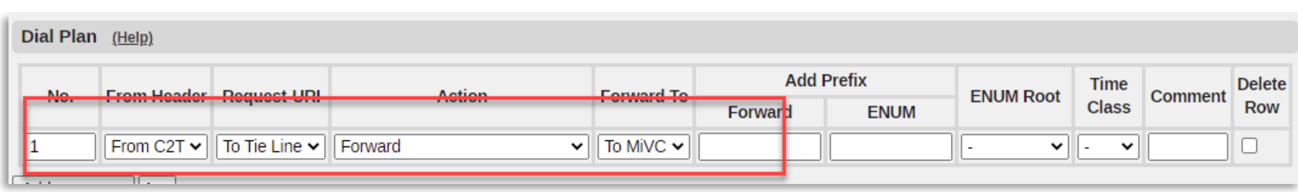
We can then define a destination (forward to) to send calls to the Trunk Switch:



Forward To (Help)

Name	No.	Use This ...	... Or This			... Or This	... Or This	Use Alias IP	Delete Row
		Account	Replacement Domain	Port	Transport	Reg Expr	Trunk		
To MiVC	1	-			-		SIP Trunk 1: Tie-Line;	-	☐

And the actual Dial Plan will look like this:



Dial Plan (Help)

No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment	Delete Row
					Forward	ENUM				
1	From C2T	To Tie Line	Forward	To MiVC			-	-		☐

2.1.10 Routing

Make sure the SIP Routing order under “SIP Traffic → Routing” looks like this:

SIP Routing Order (Help)

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

This will assure any request received for any of the registered extensions will immediately be routed as the current registration and location without reaching the dial plan. Dial Plan purpose in the use case is strictly designed to route calls to MiVC and manipulate Caller ID for calls going to Call2Teams.

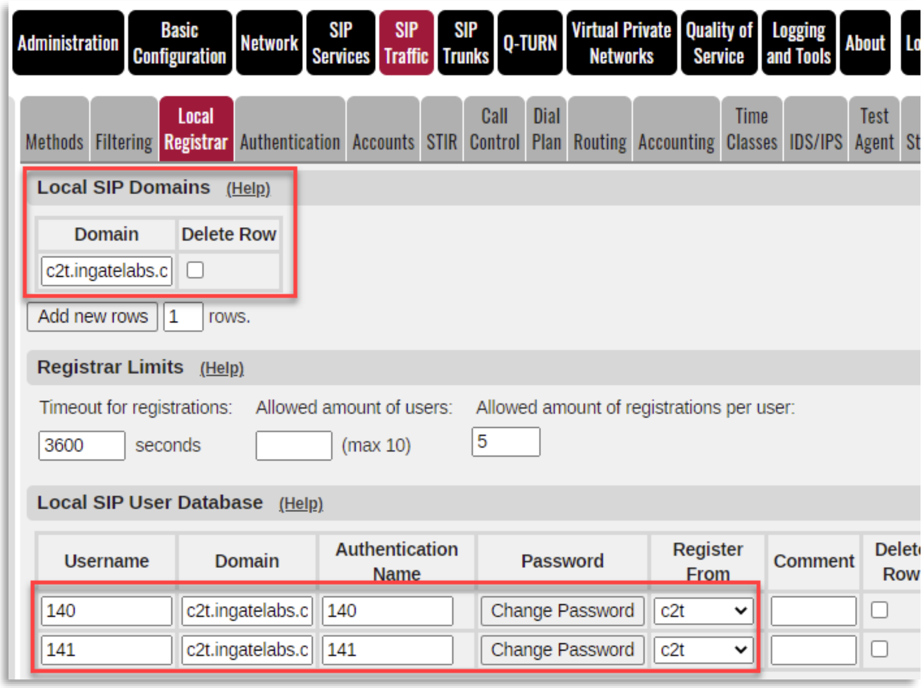
2.1.11 Local Registrar and Domain.

In this section we will setup the extension numbers, credentials and Domain for the Teams Users connected via Call2Teams.

Let's refresh the Teams user table:

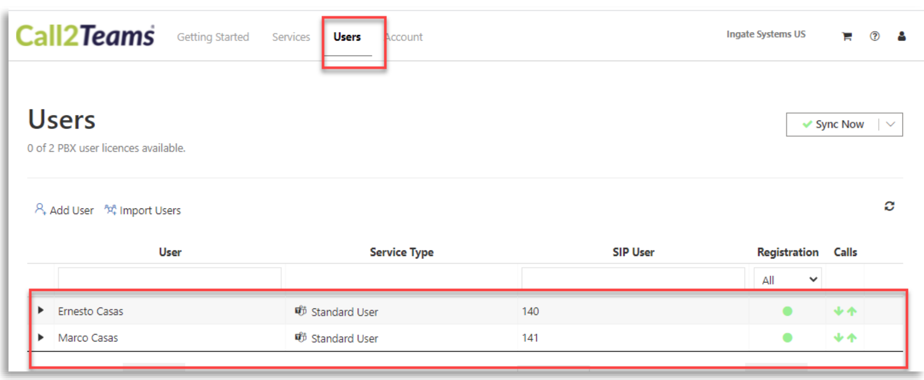
Teams User	Teams DID	SIP User for C2T
Ernesto Casas (ersnesto@ingatelabs.com)	+19547372001	140
Marco Casas (marco@ingatelabs.com)	+19547372023	141

We will later explain, for the purpose of this example, we have defined a range of extensions for Teams Users to be identified as OSE (Off System Extensions), which is required for tie-Line connections in MiVC. The range of extensions we decided was 140 – 149.

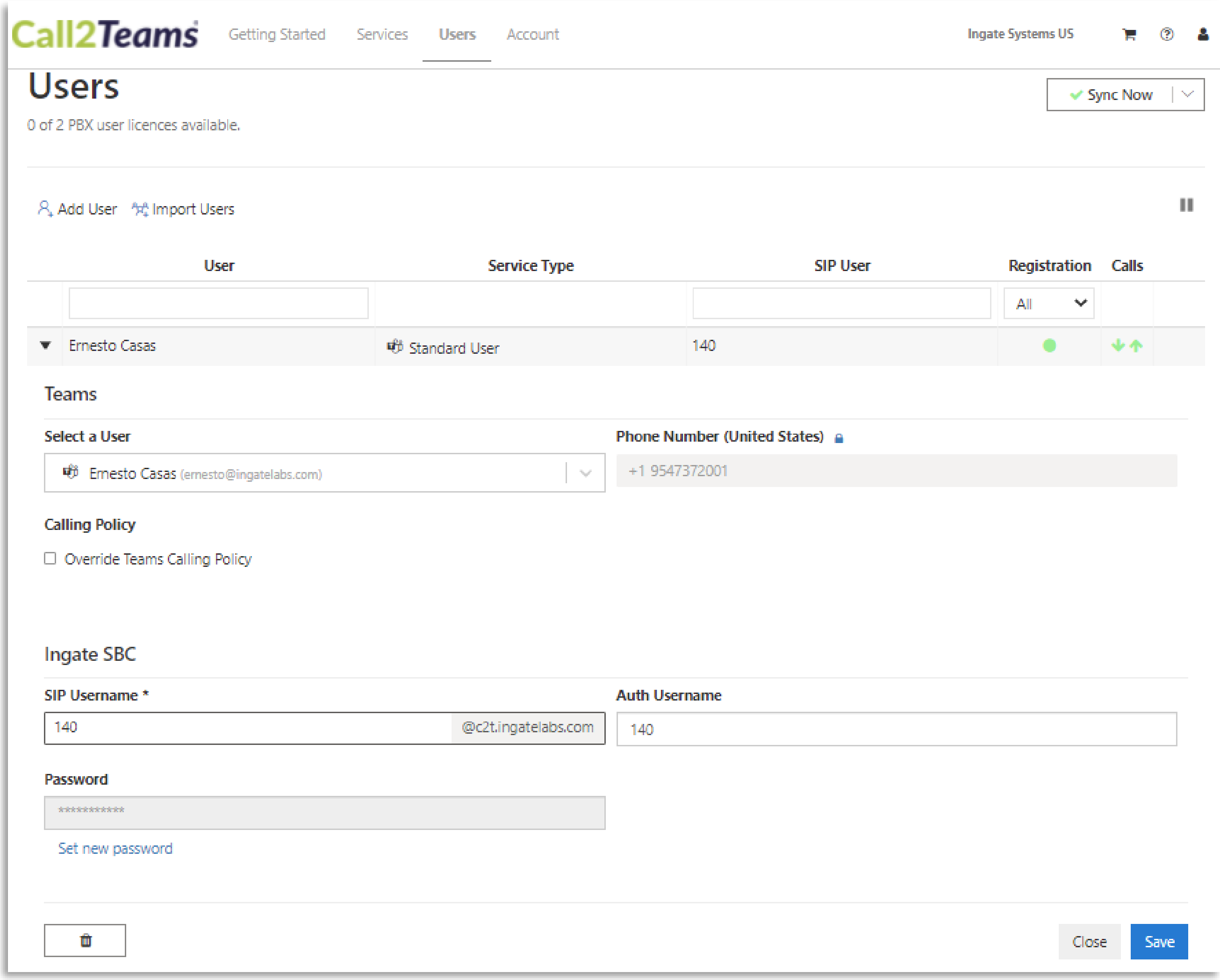


Notice the Local Domain assignment to make sure that any traffic to c2t.ingatelabs.com is locally managed.

We limit registrations only coming from C2T networks. We create one entry per Teams User in the Local SIP User Database, and assig an authentication ID and Password to be used when configuring your Call2Teams account under the Users section (Call2Teams dashboard):

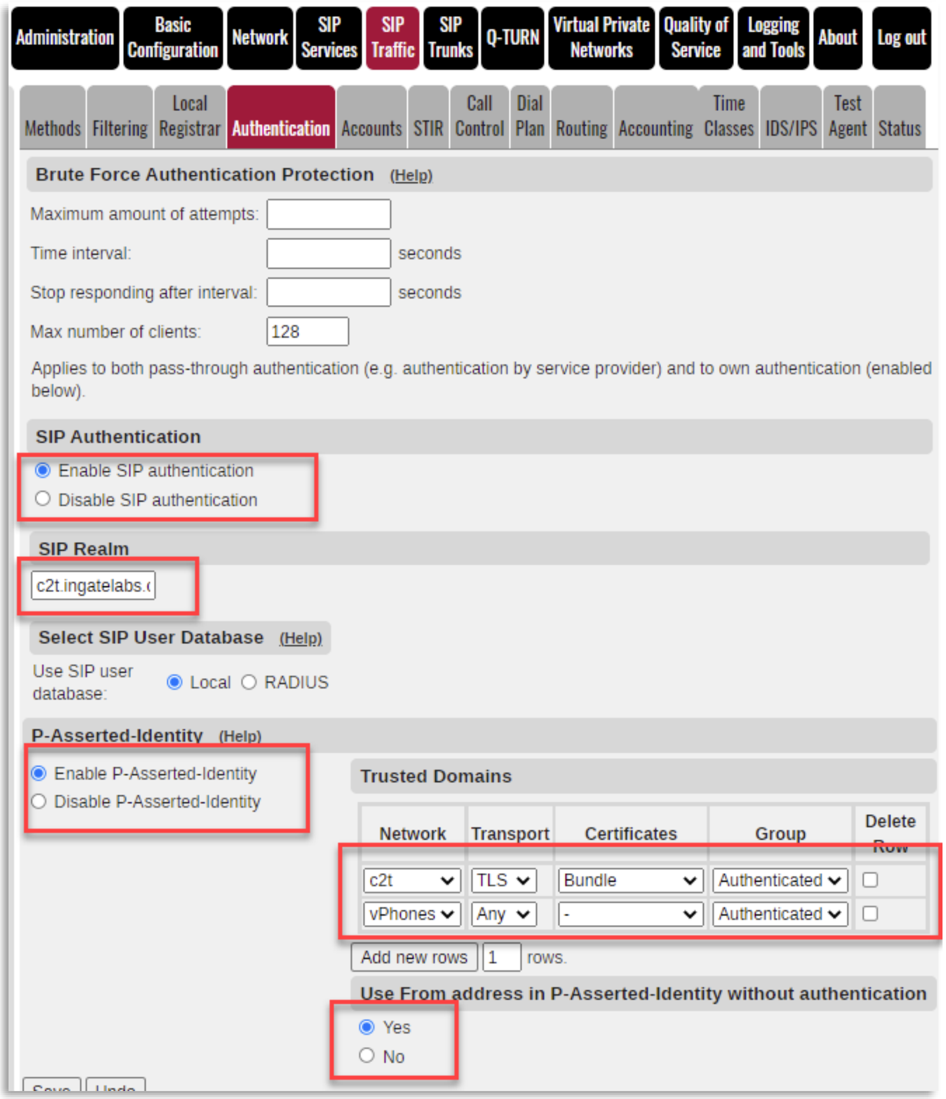


Here an example on how the user configuration looks like in Call2teams dashboard:


Call2Teams
Getting Started
Services
Users
Account
Ingate Systems US
Users
Sync Now
0 of 2 PBX user licences available.
Add User
Import Users
User
Service Type
SIP User
Registration
Calls
All
Ernesto Casas
Standard User
140
Teams
Select a User
Phone Number (United States)
Ernesto Casas (ernesto@ingatelabs.com)
+1 9547372001
Calling Policy
Override Teams Calling Policy
Ingate SBC
SIP Username *
Auth Username
140
@c2t.ingatelabs.com
140
Password
Set new password
Close
Save

Next step will be to enable authentication and the use of P-Asserted-Identity.

Go to SIP Traffic → Authentication and enable SIP authentication, as well as P-Asserted-Identity:



1) Enable SIP authentication to activate the authentication of registering users.
2) Use as SIP Realm the same domain we already created.
3) Enable P-Asserted-Identity
4) Declared as trusted Domains c2t Network and vPhones Network. For c2t as in our example we have enabled TLS select the CA Bundle certificates we created at the beginning.
5) Both will be qualified as Authenticated Groups.

3 Mitel MiVC configuration considerations

This Section explain the minimum pieces to be configured in order to enable a Tie Trunk Group between MiVC Connect and SIParator. It doesn't pretend to be a detailed configuration guide.

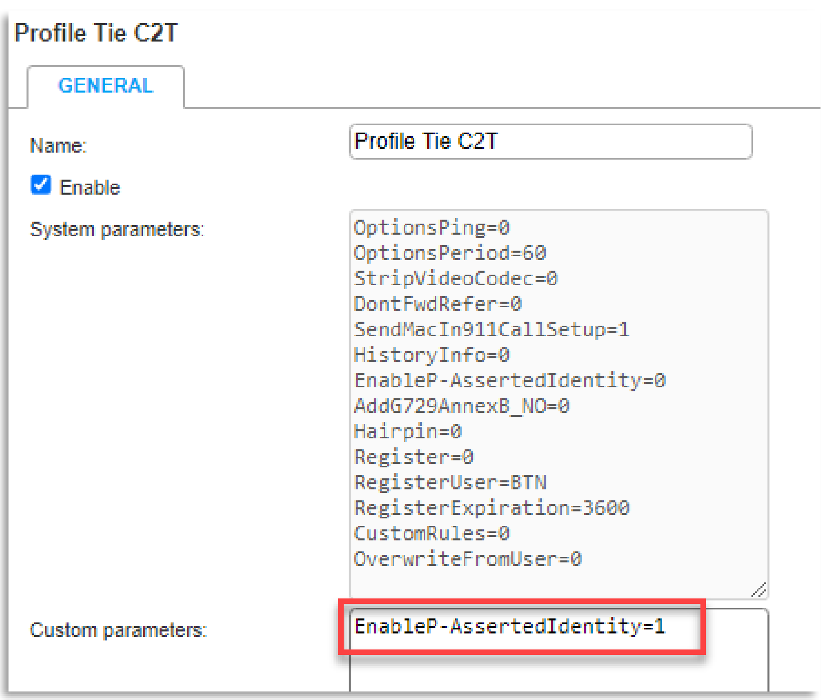
For our Lab we are using Mi Voice Connect 19.2 (Build 22.17.1600.0)

3.1 Trunk Profile for Tie Line.

Under Administration → Trunks → SIP Profiles, create a Profile copying the "Default Tie Trunk Profile". Let's call it "Profile Tie C2T".

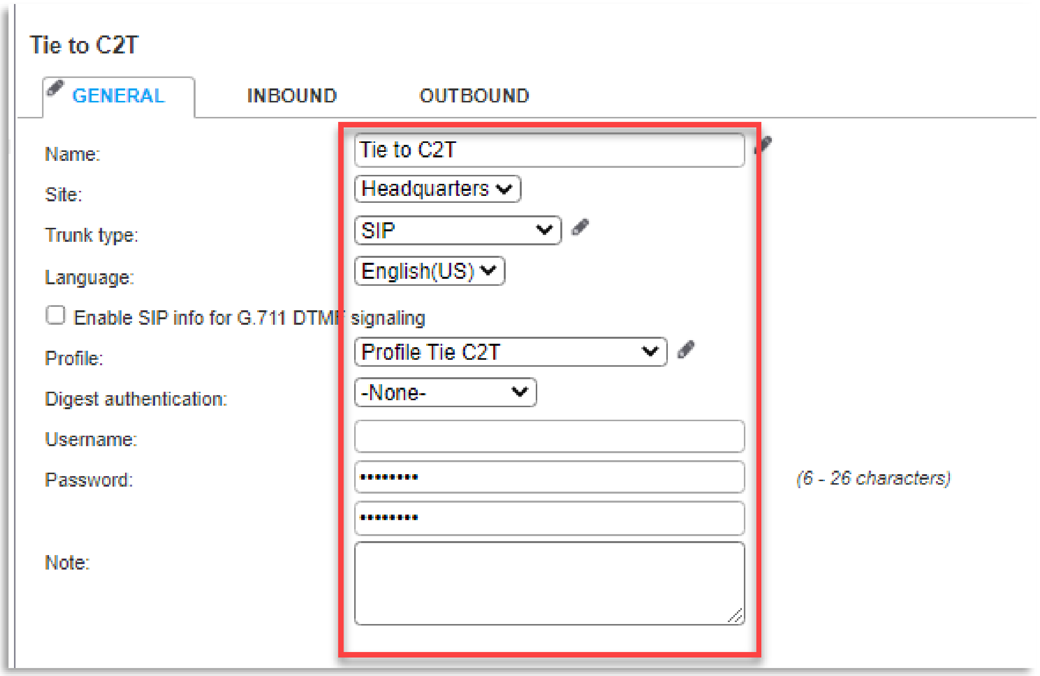
Add as a custom parameter "EnableP-AssertedIdentity=1"

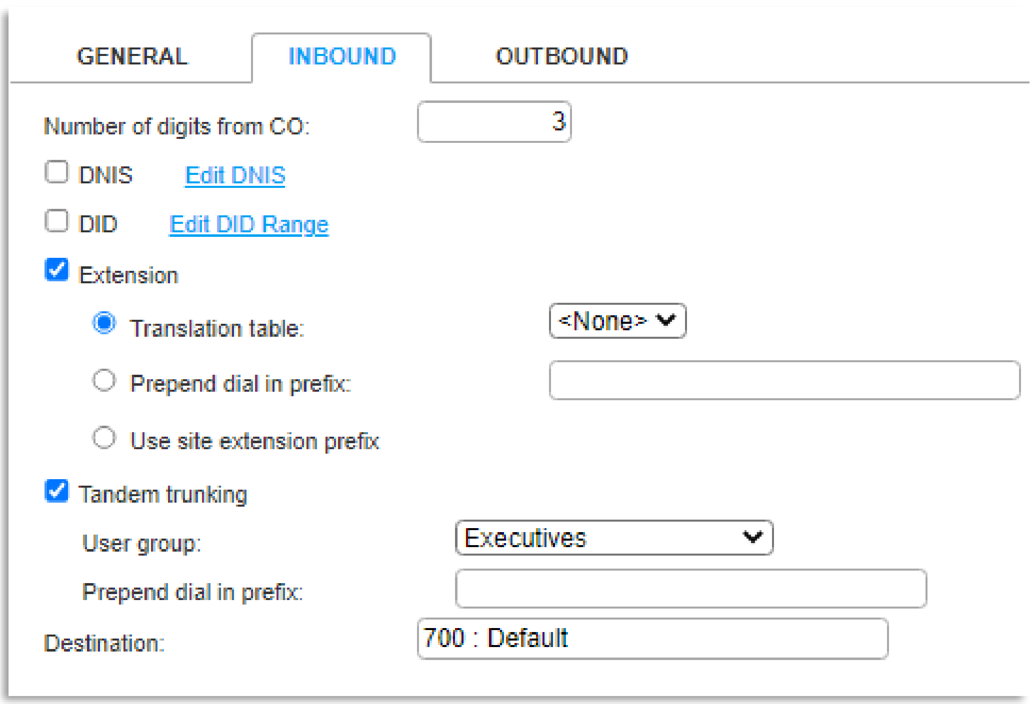
It should look like this:

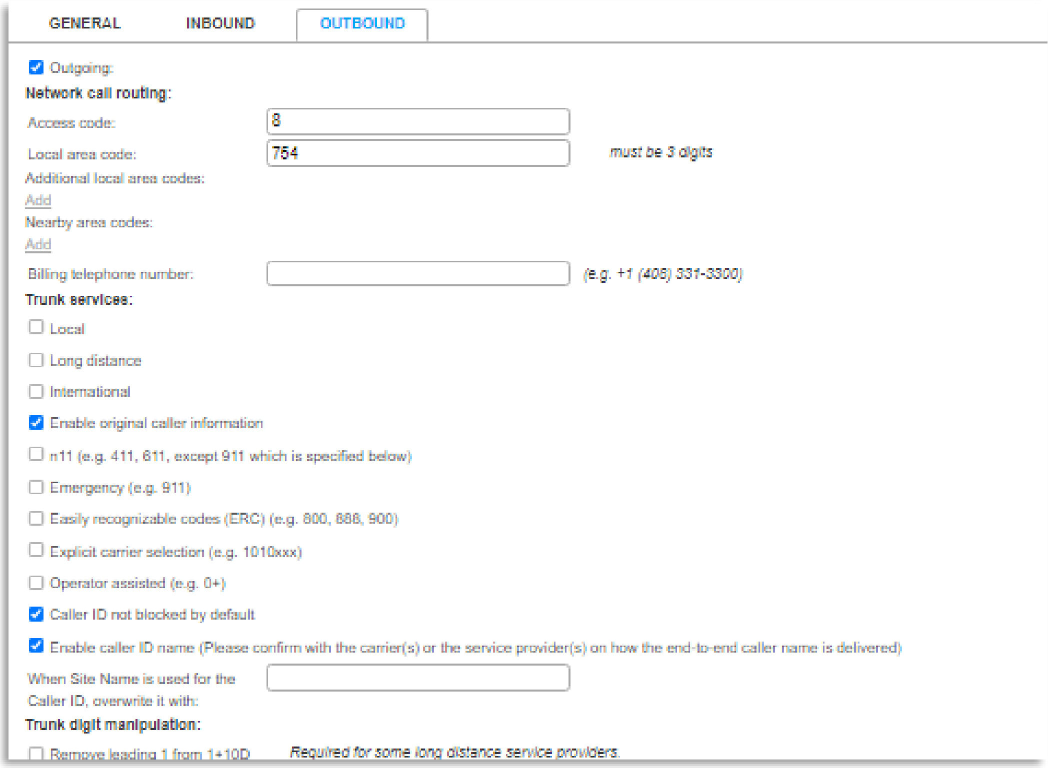


3.2 Trunk Group

Create a Trunk Group, and lest call it "Tie to C2T"

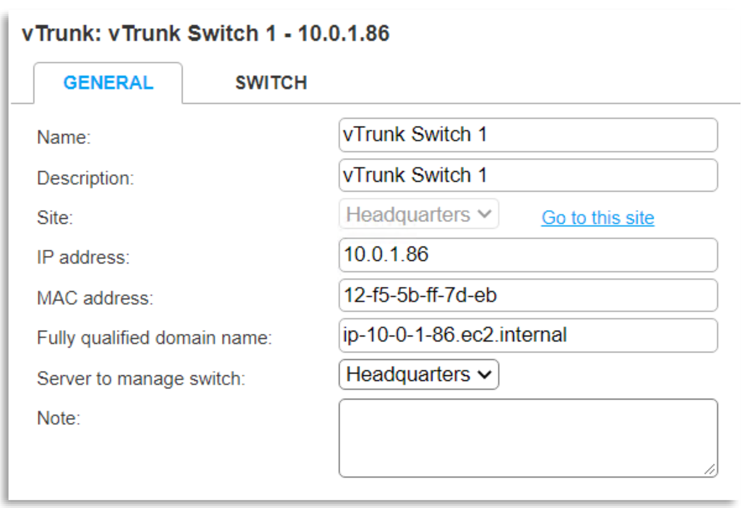






3.3 Trunk Switch

In our use case lab we have selected a vTrunk Switch to allocate the capacity for the Tie Trunk.

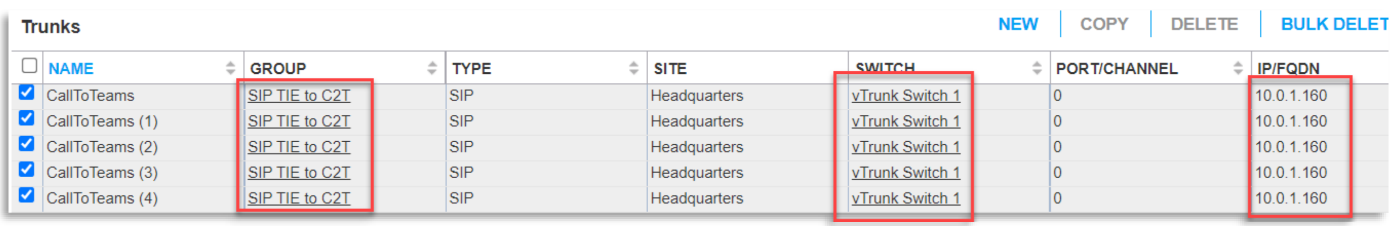


Notice this is the Switch at 10.0.1.86 we are pointing the Trunk Group in the SIParator configuration.

3.4 Assign Trunks

Create and assign your trunks (in our case we are allocating 5 trunks)

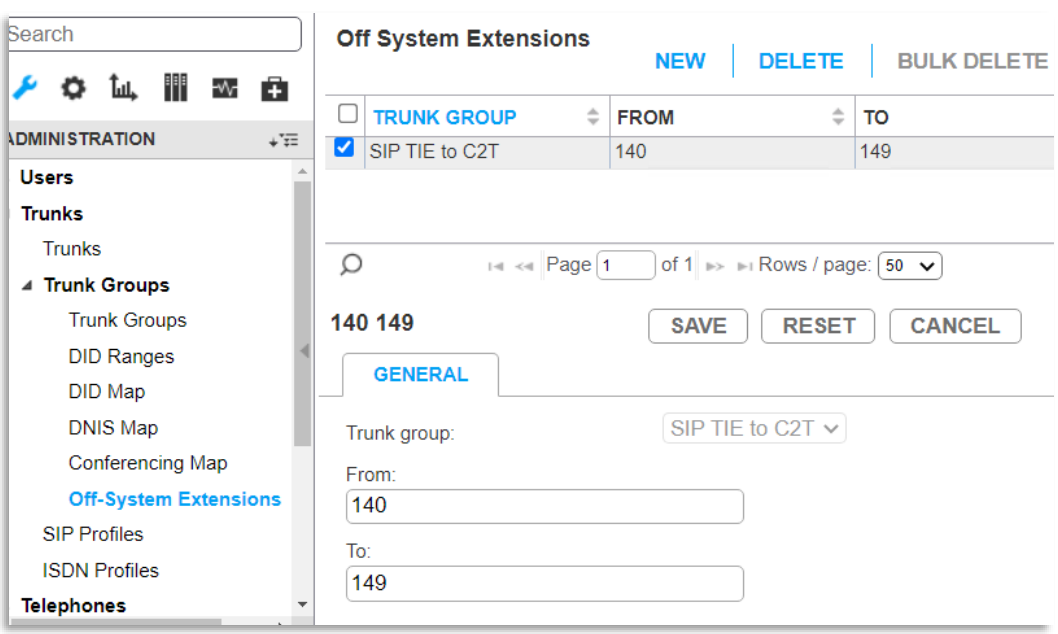
Under Administration → Trunks → Trunks and point them to the SIParator Inside IP address (10.0.1.160):



NAME	GROUP	TYPE	SITE	SWITCH	PORT/CHANNEL	IP/FQDN
CallToTeams	SIP TIE to C2T	SIP	Headquarters	vTrunk Switch 1	0	10.0.1.160
CallToTeams (1)	SIP TIE to C2T	SIP	Headquarters	vTrunk Switch 1	0	10.0.1.160
CallToTeams (2)	SIP TIE to C2T	SIP	Headquarters	vTrunk Switch 1	0	10.0.1.160
CallToTeams (3)	SIP TIE to C2T	SIP	Headquarters	vTrunk Switch 1	0	10.0.1.160
CallToTeams (4)	SIP TIE to C2T	SIP	Headquarters	vTrunk Switch 1	0	10.0.1.160

3.5 Off-System Extensions

Create an OSE (Off-System Extension) list. In our case extensions 140 – 149 will be considered OSE and associated it to the recently created Trunk Group (SIP Tie to C2T).

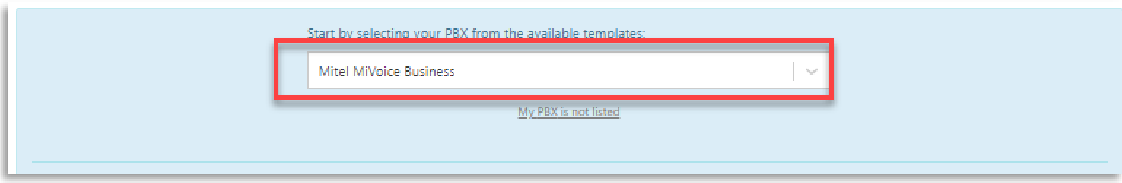


4 Call2Teams Configuration

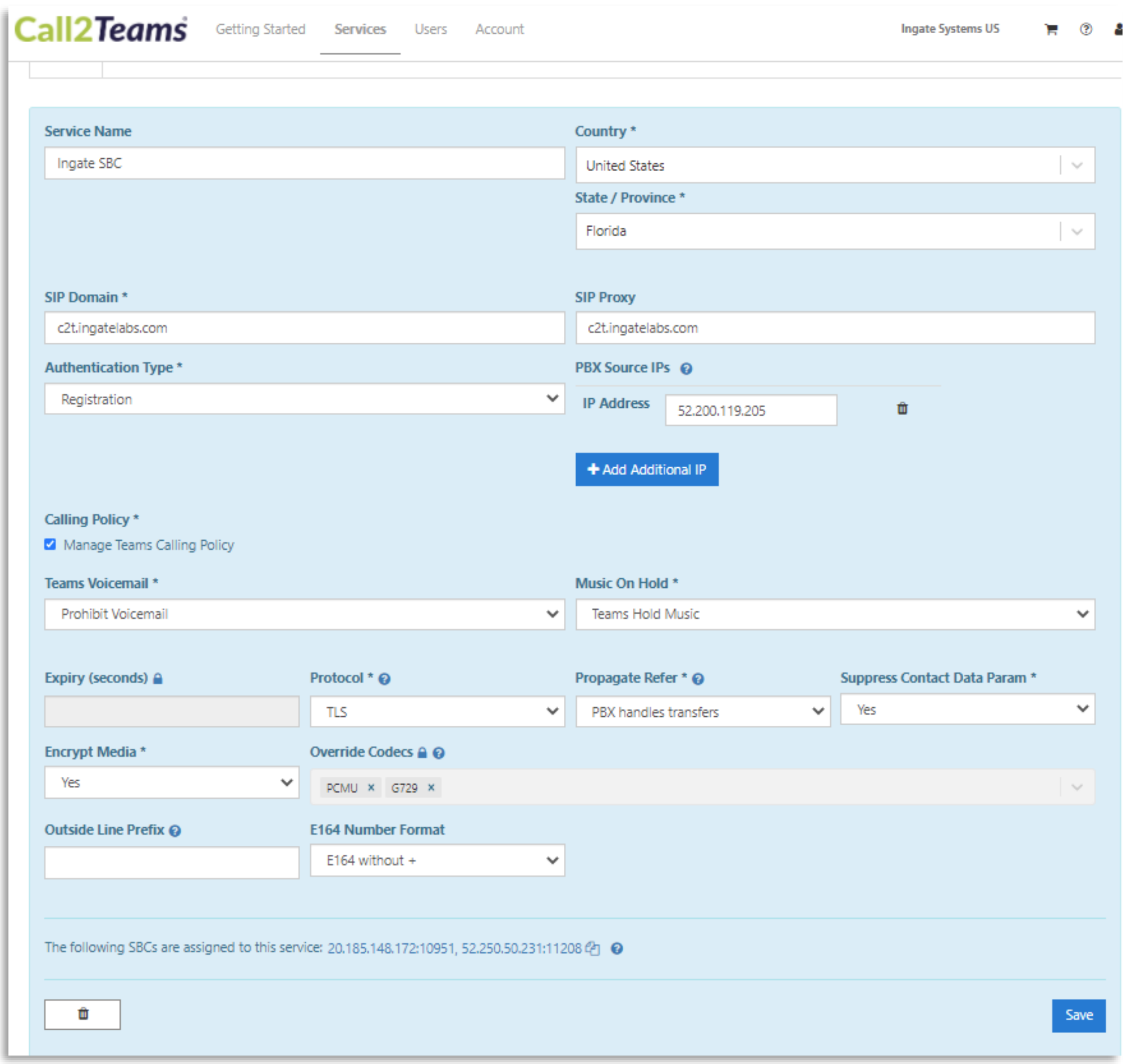
In this section we will provide screenshot samples of the sections that needs to be setup. This includes PBX and Users.

The PBX Section corresponds to the parameters needed to establish the connection and attributes of the SIParator SBC.

Add a PBX and Select “Mitel MiVoice Business”



Here is the parameters we used for the Lab and PoC:



5 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.