



# Setting up Ingate's SIParator<sup>®</sup> / Firewall<sup>®</sup>

*For*



Powering connections

MiVoice Connect

&



## Using Tie Lines

For Ingate SIParators using software release 6.3.2 or later

Revision 1.0  
August 2021

# Table of Contents

<b>Table of Contents .....</b>	<b>2</b>
<b>1 Minimum Requirements.....</b>	<b>3</b>
1.1 SIParator Version .....	3
1.2 Ingate Licensing.....	3
1.3 Call2Teams Account. ....	3
1.4 FQDN/Public IP for the SBC.....	3
1.5 Public Trusted certificate. ....	3
1.6 MS Teams Requirements. ....	4
<b>2 SIParator configuration.....</b>	<b>5</b>
2.1 Topology with SIParator in the DMZ, IPPBX on LAN and ITSP on WAN.....	5
2.1.1 Requirements .....	5
2.1.2 SBC Domain / FQDN.....	6
2.1.3 Deploy CA Certificates and Configure SIParator TLS Certificate (If needed). ....	6
2.1.4 SIParator Network configuration.....	11
2.1.5 Configure SIP Signaling .....	13
2.1.6 Configure Media Encryption.....	15
2.1.7 Other Media related configuration .....	16
2.1.8 Tie Trunk Configuration .....	18
2.1.9 Dial Plan .....	20
2.1.10 Routing.....	21
2.1.11 Local Registrar and Domain. ....	22
<b>3 Mitel MiVC configuration considerations.....</b>	<b>26</b>
3.1 Trunk Profile for Tie Line.....	26
3.2 Trunk Group.....	27
3.3 Trunk Switch .....	28
3.4 Assign Trunks .....	29
3.5 Off-System Extensions.....	29
<b>4 Call2Teams Configuration .....</b>	<b>30</b>
<b>5 Additional help or support .....</b>	<b>31</b>

# 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 simultaneous 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](mailto: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](mailto: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](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](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](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.

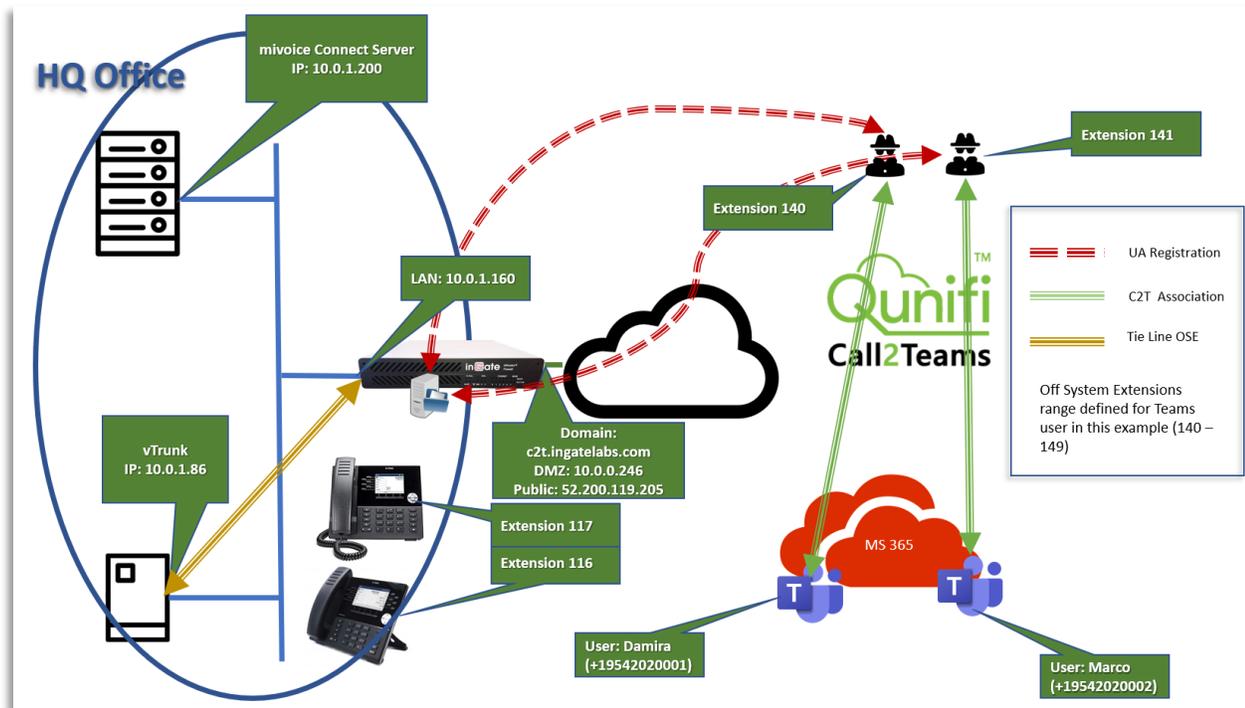
## 1.6 MS Teams Requirements.

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:

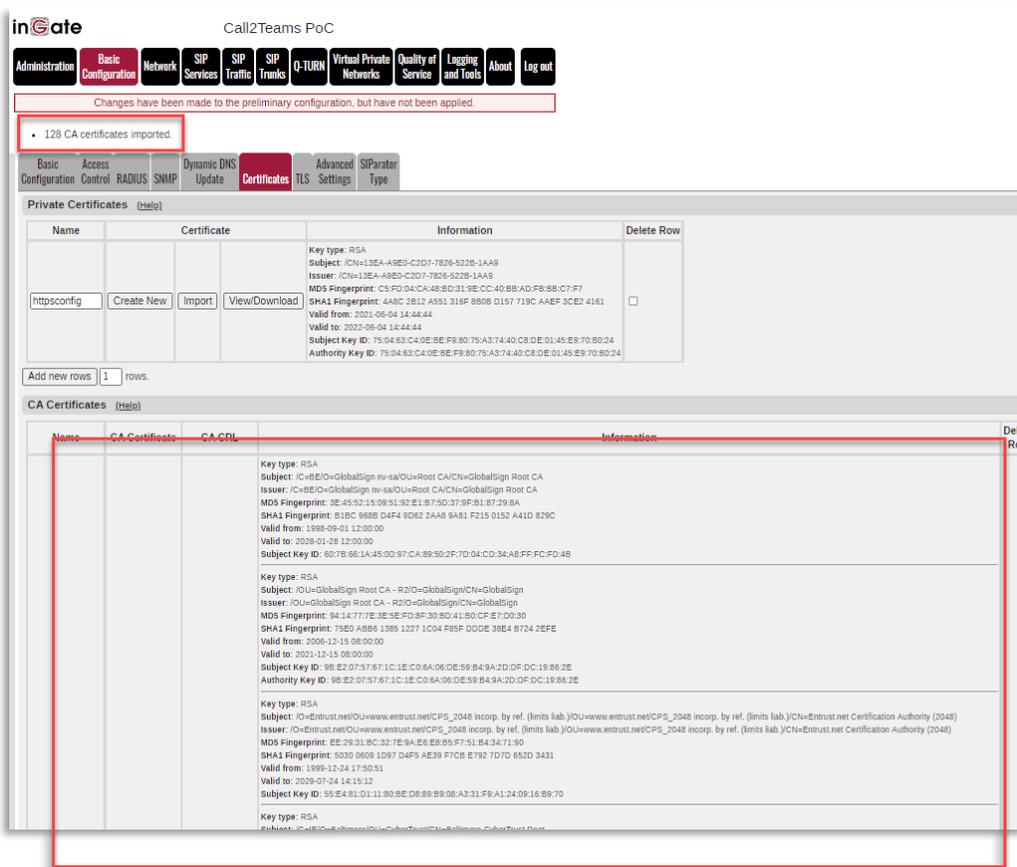
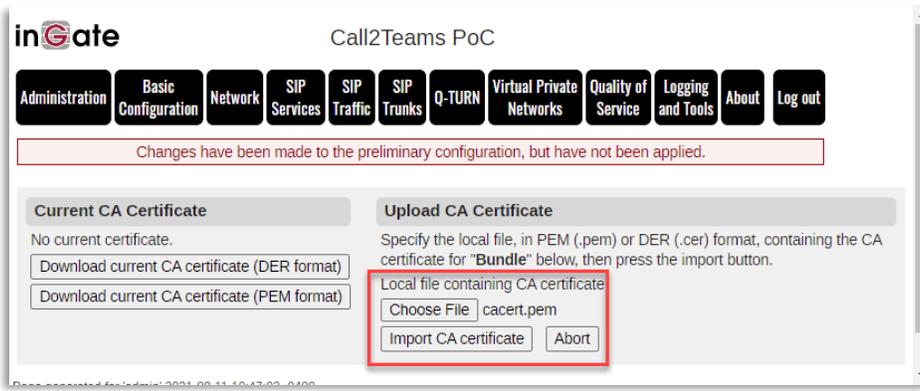
Teams User	Teams DID	SIP User for C2T
Ernesto Casas (ersnesto@ingatelabs.com)	+19547372001	140
Marco Casas (marco@ingatelabs.com)	+19547372023	141

### 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:



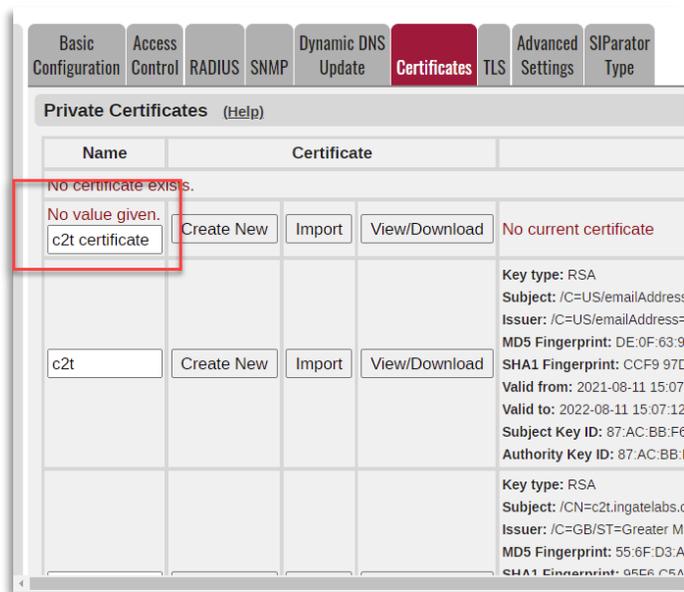
Import pem certificates bundle into SIParator CA Certificates:



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”

**ingate** Call2Teams PoC

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

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

**Current Certificate**  
No current certificate.

**Create Certificate or Certificate Request**  
Fill in the certificate data for "c2t certificate" 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

Expire in (days):  Country code (C):  Organization (O):

**Common Name (CN):**  State/province (ST):  Organizational Unit (OU):

Email address:  Locality/town (L):

**SubjectAltName Extension**  
Enter the alternative names that you want to add to a certificate or a certificate request. Multiple values can be added by using comma separation.  
Email:   
URI:   
DNS:   
IP:

**Key Length and Signature Algorithm**  
Select the key length and the signature algorithm that you want to use when creating a certificate or a certificate request.  
Key length (bits):   
Signature algorithm:

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

Fields marked with "\*" are mandatory.

Page generated for 'admin' 2021-08-11 17:51:56 -0400.  
Software SIParator/Firewall 6.3.3. Copyright © 2021 Ingate Systems AB.

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.

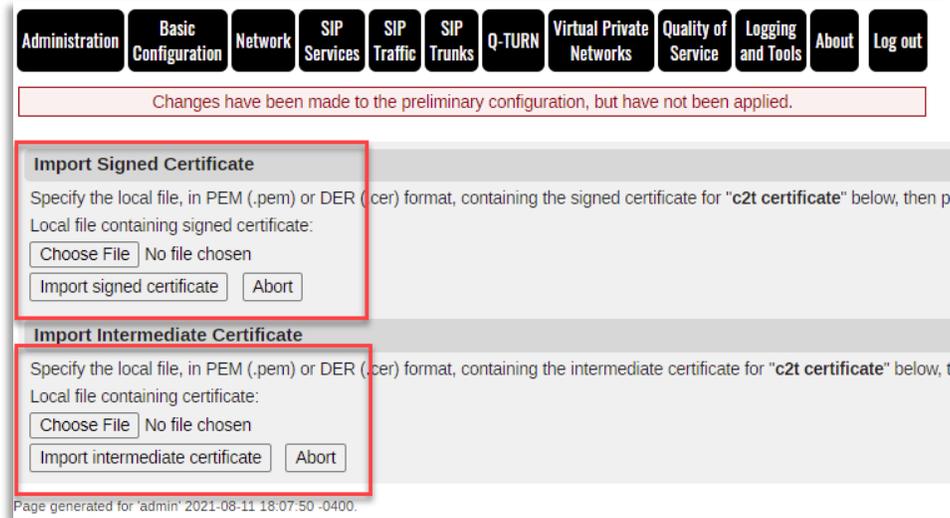
Click on download certificate/certificate request (PEM format)

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](mailto: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:

The screenshot shows the InGate configuration interface for 'Call2Teams PoC'. The 'Network' tab is selected, and the 'All Interfaces' sub-tab is active. The 'Interface Overview' section contains a table with the following data:

Physical Device	Interface Name	Active	MTU
eth0	outside	Yes	1500
eth1	inside	Yes	1500

Below this, the 'Directly Connected Networks' section shows a table with the following data:

Name	Address Type	DNS Name or IP Address	IP Address	Netmask / Bits	Network Address	Broadcast Address	Interface or Tunnel	VLAN Id
outside	DHCP		*		-	-	outside (eth0)	
inside	DHCP		*		-	-	inside (eth1)	

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:

**inGate** Call2Teams PoC

Administration Basic Configuration **Network** SIP Services SIP Traffic SIP Trunks Q-TURN Virtual Private Networks Quality of Service Logging and Tools About Log out

Networks and Computers Default Gateways All Interfaces VLAN Eth0 Eth1 Interface Status PPPoE Tunnels Topology

Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/VLAN	Delete Row
		DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address		
+ c2t	-	20.185.148.172	20.185.148.172			outside (eth0 untagged)	<input type="checkbox"/>
	-	52.250.50.231	52.250.50.231			outside (eth0 untagged)	<input type="checkbox"/>
+ vPhones	-	10.0.1.0	10.0.1.0	10.0.1.255	10.0.1.255	inside (eth1 untagged)	<input type="checkbox"/>

Add new rows 1 groups with 1 rows per group.

Save Undo Look up all IP addresses again

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

Outside Line Prefix **E164 Number Format**

E164 without +

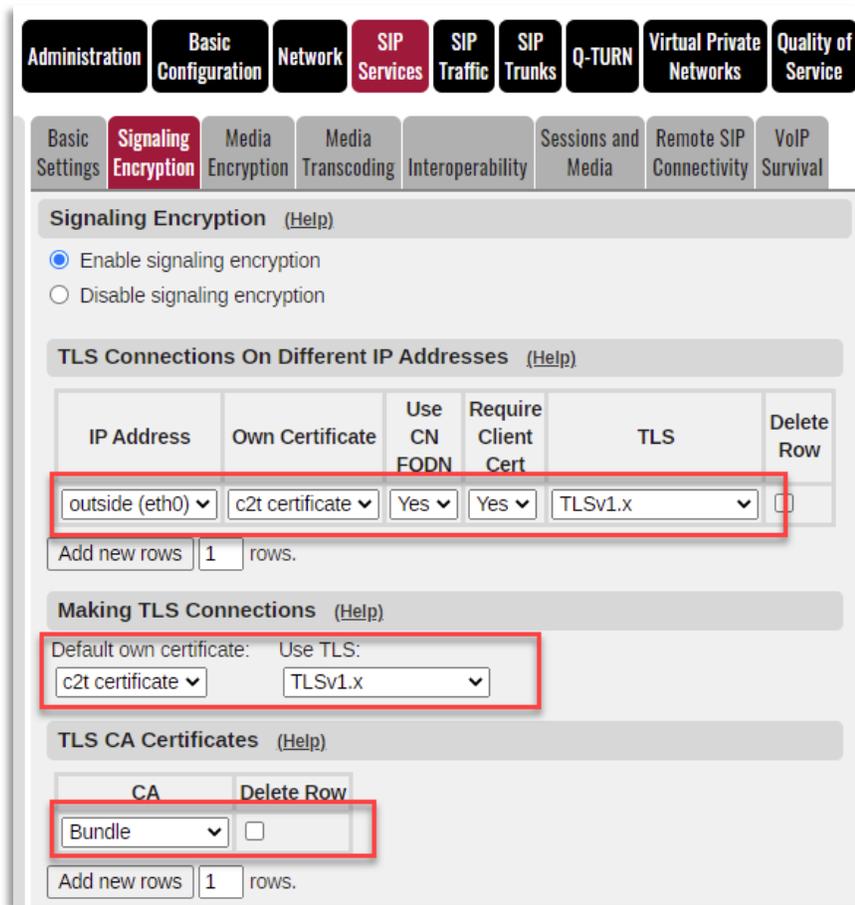
The following SBCs are assigned to this service: 20.185.148.172:10951, 52.250.50.231:11208

Save

- **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)

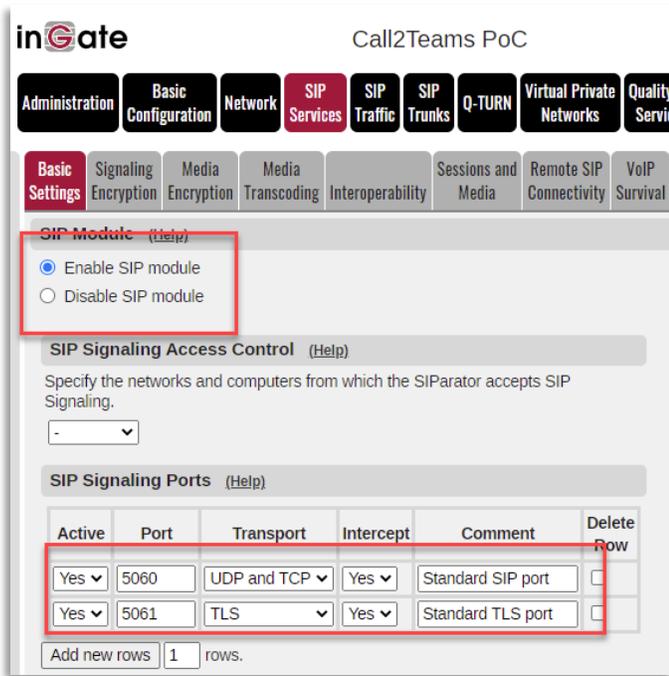
Select TLSv1.x in the TLS column.

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.

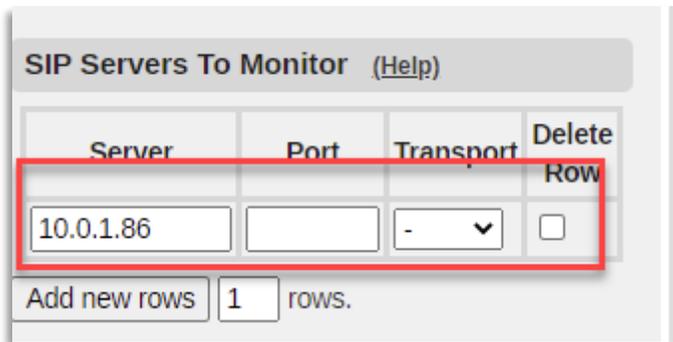
### 2.1.5 Configure SIP Signaling

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.

Public IP Address for NATed SIParator	
DNS Name or IP Address	IP Address
c2t.ingatelabs.com	52.200.119.205

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:

The screenshot shows the InGate SBC configuration interface. The top navigation bar includes 'Administration', 'Basic Configuration', 'Network', 'Rules and Relays', and 'SIP Services'. The 'SIP Services' menu is expanded to show sub-options: 'Basic Settings', 'Signaling Encryption', 'Media Encryption', 'Media Transcoding', and 'Interoperability'. The 'Media Encryption' sub-option is selected and highlighted with a red box. Below this, the 'Media Encryption' configuration page is visible, featuring a red-bordered box around the 'Enable media encryption' radio button, which is selected. The 'Disable media encryption' radio button is also visible but unselected.

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

Basic Settings Signaling Encryption **Media Encryption** Media Transcoding Interoperability Sessions and Media Remote SIP Connectivity VoIP Survival

**Media Encryption** (Help)

Enable media encryption  
 Disable media encryption

**SIP Media Encryption Policy** (Help)

No.	Network	Transport	Suite Requirements	Allow Transcoding	Delete Row
1	c2t	TLS	SRTP	Yes	<input type="checkbox"/>

Add new rows  rows.

**Default Encryption Policy** (Help)

Suite requirements:

Allow transcoding:  Yes  No

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**.

**Add Cryptos in the B2BUA** (Help)

Add cryptos in the B2BUA:  Yes  No

### 2.1.7 Other Media related configuration

Administration Basic Configuration Network Rules and Relays SIP Services SIP Traffic SIP Trunks Q-TURN Failover Virtual Private Networks

Basic Settings Signaling Encryption Media Encryption Media Transcoding Interoperability Sessions and Media Remote SIP Connectivity VoIP Survival

### Session Configuration

Session timer: 14400 seconds Allowed amount of concurrent sessions (leave blank for no limit): [ ] (max 40)

Timeout for SIP over TCP/TLS: 90 seconds

#### Media Proxy (Help)

Enable Media Proxy  
 Disable Media Proxy

Always use the Media Proxy:  
 Yes  No

#### Media Configuration (Help)

Limitation of sender of media streams:  
 Lock IP address and port to first sender  
 Only allow receiving IP address, but multiple ports  
 Allow multiple sender IP addresses and ports

Allowed number of senders: 10

Allowed amount of media streams per SIP session: 6

Support forked media streams:  
 Yes  No

#### Always Relay Media (Help)

Always relay media:  Yes  No

Timeout for one-way media streams: [ ] seconds

Tear down media streams at RTP/RTCP timeouts:  
 Yes  No

Timeout for RTP streams: [ ] seconds

Timeout for RTCP streams: [ ] seconds

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

The screenshot shows the InGate configuration interface for Call2Teams PoC. The 'SIP Traffic' menu item is highlighted. The 'Filtering' sub-menu is active, showing the 'Sender IP Filter Rules' section. This section contains a table with two rows, both with 'Process all' as the action and 'Reject all' as the default policy. Below this, the 'Preloaded Route Rules' section shows a 'Reject' default policy. The 'Allowed Origins for SIP over WebSocket' section has one row. The 'Policy for Signaling and Media on different Networks' section has 'Allow Signaling and Media on different Networks' selected. The 'Content Type Filter Rules' section is partially visible at the bottom.

No.	From Network	Action	Delete Row	Default Policy For SIP Requests
1	c2t	Process all	<input type="checkbox"/>	<input type="radio"/> Process all <input type="radio"/> Local only <input checked="" type="radio"/> Reject all
2	vPhones	Process all	<input type="checkbox"/>	<input type="radio"/> Process all <input type="radio"/> Local only <input checked="" type="radio"/> Reject all

No.	From Network	Action	Delete Row	Default Policy For Preloaded Routes
				<input checked="" type="radio"/> Reject <input type="radio"/> Authenticate <input type="radio"/> Remove <input type="radio"/> Allow

Scheme	Host	Port	Delete Row

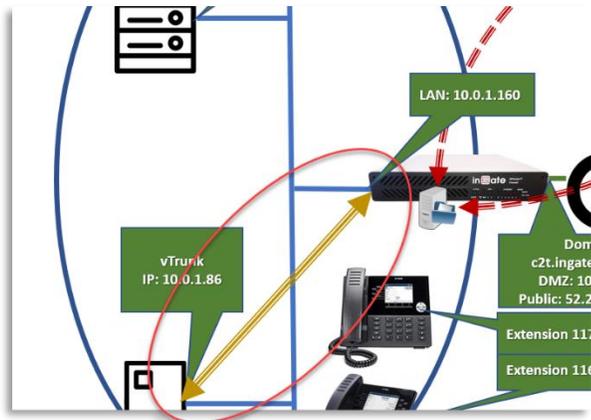
Allow Signaling and Media on different Networks  
 Reject Signaling and Media on different Networks

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 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.

**SIP Trunking Service** (Help)

Use parameters from other SIP trunk

Define SIP trunk parameters

Service name:  (Unique descriptive name)

Service Provider Domain:  (SQDN or IP address)

Restrict to calls from:  (No restriction)

Outbound Proxy:  (SQDN or IP address)

Use alias IP address:  (Forces this source address from our side)

Outbound Gateway:  (Use Default Gateway)

Signaling Transport:  (Automatic)

Port number:

From header domain:

Host name in Request-URI of incoming calls:  (Trunk ID - Domain name)

Remote Trunk Group Parameters (RFC 4904):

Used as:  (Don't use TGP)

Local Trunk Group Parameters (RFC 4904):

Used as:  (Don't use TGP)

Preserve Max-Forwards:

Relay media:

Exactly one Via header:

'gin' registration (RFC 6140):

Hide Record-Route:

Show only one To tag:

SIP 3xx redirection to provider domain:

SIP 3xx redirection to caller domain:

Route incoming based on:

Service Provider domain is trusted:  (For P-Asserted-Identity)

Use P-Preferred-Identity:  (Instead of P-Asserted-Identity)

Forward outgoing REFER:

Refer-To header domain:

Send DTMF via SIP INFO:

Remove video:

Max simultaneous calls:  (Call Admission Control)

Max simultaneous calls per Trunk Line:

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**)

The screenshot shows three configuration sections: Main Trunk Line, PBX Lines, and SIP Lines. Each section has a table with columns for No., Reg., and various call parameters. In the SIP Lines section, the 'From SIP Number/User' field contains '(\*)', 'Display Name' is 'Teams \$1', 'User Name' is '\$1', 'Incoming Trunk Match' is '(\*)', and 'Forward to SIP Account' is 'sip.\$1@c2t.ingatelab.com'. The 'Main Trunk Line' section shows 'User Name' as 'NA'. The 'PBX Lines' section is currently empty.

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 From 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.

The screenshot shows the 'Setup for the PBX' configuration section. It has two radio buttons: 'Use PBX from other SIP trunk' (which is selected) and 'Define PBX settings'. Below the radio buttons is a dropdown menu labeled 'PBX from:' with a downward arrow.

### 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, it 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](http://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	<input type="checkbox"/>

Add new rows | 1 rows.

---

**Matching Request-URI** (Help)

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

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		Use Alias IP	Delete Row
		Account	Replacement Domain	Port	Transport	Reg Expr	Trunk		
To MiVC	1	-			-		SIP Trunk 1: Tie-Line;	<input type="checkbox"/>	

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			-	-		<input type="checkbox"/>

### 2.1.10 Routing

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

SIP Routing Order <a href="#">(Help)</a>	
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.

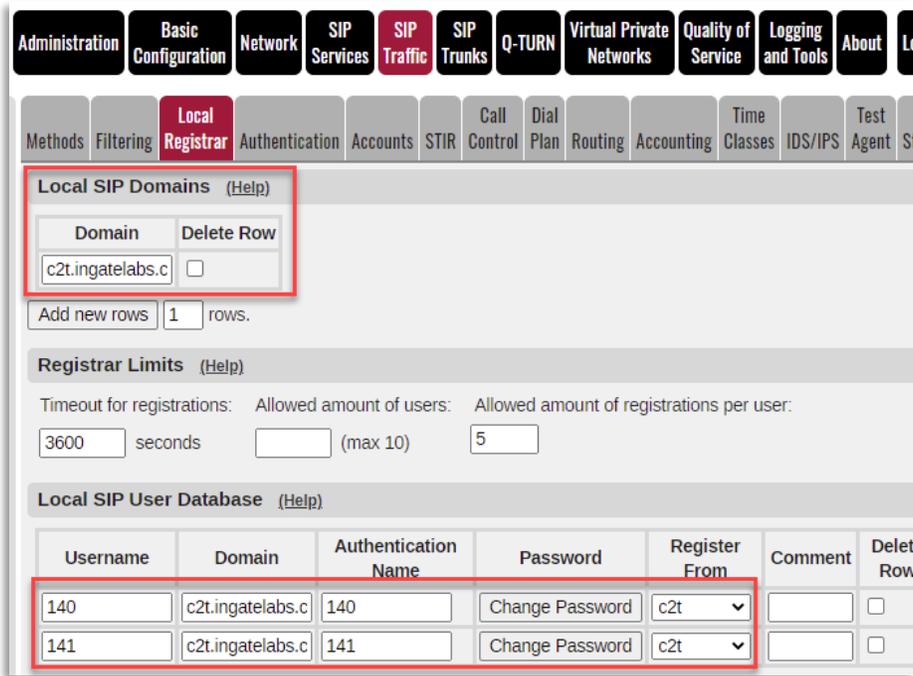
### 2.1.11 Local Registrar and Domain.

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

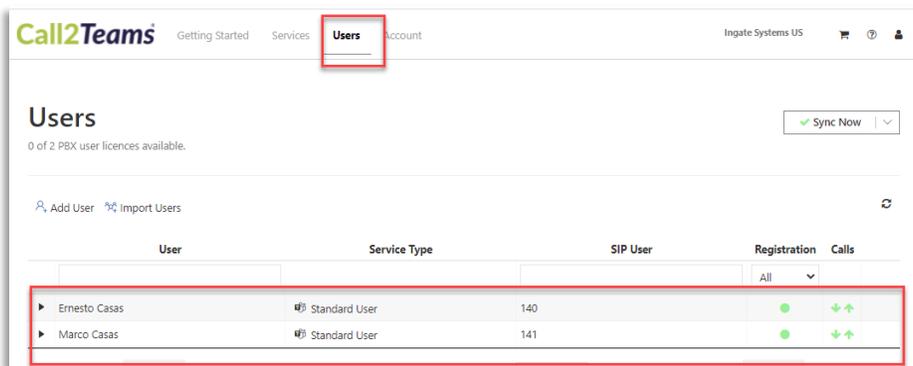
Let's refresh the Teams user table:

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 assign 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:

# Users

Sync Now

0 of 2 PBX user licences available.

Add User Import Users

User	Service Type	SIP User	Registration	Calls
<input type="text"/>		<input type="text"/>	All	
Ernesto Casas	Standard User	140	<span style="color: green;">●</span>	<span style="color: green;">↕</span>

## Teams

Select a User

Ernesto Casas (ernesto@ingatelabs.com)

Phone Number (United States)

+1 9547372001

Calling Policy

Override Teams Calling Policy

## Ingate SBC

SIP Username \*

140@c2t.ingatelabs.com

Auth Username

140

Password

\*\*\*\*\*

Set new password

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:

**Brute Force Authentication Protection** (Help)

Maximum amount of attempts:

Time interval:  seconds

Stop responding after interval:  seconds

Max number of clients:

Applies to both pass-through authentication (e.g. authentication by service provider) and to own authentication (enabled below).

**SIP Authentication**

Enable SIP authentication  
 Disable SIP authentication

**SIP Realm**

**Select SIP User Database** (Help)

Use SIP user database:  Local  RADIUS

**P-Asserted-Identity** (Help)

Enable P-Asserted-Identity  
 Disable P-Asserted-Identity

**Trusted Domains**

Network	Transport	Certificates	Group	Delete Row
c2t	TLS	Bundle	Authenticated	<input type="checkbox"/>
vPhones	Any	-	Authenticated	<input type="checkbox"/>

Add new rows  rows.

**Use From address in P-Asserted-Identity without authentication**

Yes  
 No

- 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:

Profile Tie C2T

**GENERAL**

Name: Profile Tie C2T

Enable

System parameters:

```
OptionsPing=0
OptionsPeriod=60
StripVideoCodec=0
DontFwdRefer=0
SendMacIn911CallSetup=1
HistoryInfo=0
EnableP-AssertedIdentity=0
AddG729AnnexB_NO=0
Hairpin=0
Register=0
RegisterUser=BTN
RegisterExpiration=3600
CustomRules=0
OverwriteFromUser=0
```

Custom parameters: EnableP-AssertedIdentity=1

## 3.2 Trunk Group

Create a Trunk Group, and let's call it "Tie to C2T"

**Tie to C2T**

**GENERAL** INBOUND OUTBOUND

Name: Tie to C2T

Site: Headquarters

Trunk type: SIP

Language: English(US)

Enable SIP info for G.711 DTMF signaling

Profile: Profile Tie C2T

Digest authentication: -None-

Username:

Password:   (6 - 26 characters)

Note:

GENERAL **INBOUND** OUTBOUND

Number of digits from CO:

DNIS [Edit DNIS](#)

DID [Edit DID Range](#)

Extension

Translation table: <None>

Prepend dial in prefix:

Use site extension prefix

Tandem trunking

User group: Executives

Prepend dial in prefix:

Destination: 700 : Default

GENERAL INBOUND **OUTBOUND**

Outgoing:

**Network call routing:**

Access code:

Local area code:  must be 3 digits

Additional local area codes:

[Add](#)

Nearby area codes:

[Add](#)

Billing telephone number:  (e.g. +1 (408) 331-3300)

**Trunk services:**

Local

Long distance

International

Enable original caller information

n11 (e.g. 411, 611, except 911 which is specified below)

Emergency (e.g. 911)

Easily recognizable codes (ERC) (e.g. 800, 888, 900)

Explicit carrier selection (e.g. 1010xxx)

Operator assisted (e.g. 0+)

Caller ID not blocked by default

Enable caller ID name (Please confirm with the carrier(s) or the service provider(s) on how the end-to-end caller name is delivered)

When Site Name is used for the Caller ID, overwrite it with:

**Trunk digit manipulation:**

Remove leading 1 from 1+10D Required for some long distance service providers.

### 3.3 Trunk Switch

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

**vTrunk: vTrunk Switch 1 - 10.0.1.86**

GENERAL SWITCH

Name:

Description:

Site:  [Go to this site](#)

IP address:

MAC address:

Fully qualified domain name:

Server to manage switch:

Note:

**vTrunk: vTrunk Switch 1 - 10.0.1.86**

GENERAL SWITCH

Max SIP trunk capacity (G.711): 500/1000 with/without advanced features. ?

SIP trunks configured:

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):

Trunks								NEW	COPY	DELETE	BULK DELETE
<input type="checkbox"/>	NAME	GROUP	TYPE	SITE	SWITCH	PORT/CHANNEL	IP/FQDN				
<input checked="" type="checkbox"/>	CallToTeams	SIP TIE to C2T	SIP	Headquarters	vTrunk Switch 1	0	10.0.1.160				
<input checked="" type="checkbox"/>	CallToTeams (1)	SIP TIE to C2T	SIP	Headquarters	vTrunk Switch 1	0	10.0.1.160				
<input checked="" type="checkbox"/>	CallToTeams (2)	SIP TIE to C2T	SIP	Headquarters	vTrunk Switch 1	0	10.0.1.160				
<input checked="" type="checkbox"/>	CallToTeams (3)	SIP TIE to C2T	SIP	Headquarters	vTrunk Switch 1	0	10.0.1.160				
<input checked="" type="checkbox"/>	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).

Search

ADMINISTRATION

- Users
- Trunks
  - Trunks
  - Trunk Groups
  - DID Ranges
  - DID Map
  - DNIS Map
  - Conferencing Map
  - Off-System Extensions
  - SIP Profiles
  - ISDN Profiles
- Telephones

**Off System Extensions** NEW DELETE BULK DELETE

<input type="checkbox"/>	TRUNK GROUP	FROM	TO
<input checked="" type="checkbox"/>	SIP TIE to C2T	140	149

140 149 SAVE RESET CANCEL

GENERAL

Trunk group: SIP TIE to C2T

From:

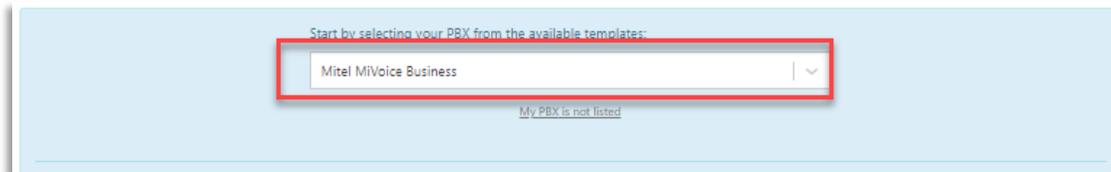
To:

## 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:

The screenshot shows the configuration page for a service named 'Ingate SBC'. The interface includes the following fields and options:

- Service Name:** Ingate SBC
- Country:** United States
- State / Province:** Florida
- SIP Domain:** c2t.ingatelabs.com
- SIP Proxy:** c2t.ingatelabs.com
- Authentication Type:** Registration
- PBX Source IPs:** 52.200.119.205 (with an '+ Add Additional IP' button)
- Calling Policy:**  Manage Teams Calling Policy
- Teams Voicemail:** Prohibit Voicemail
- Music On Hold:** Teams Hold Music
- Expiry (seconds):** (empty field)
- Protocol:** TLS
- Propagate Refer:** PBX handles transfers
- Suppress Contact Data Param:** Yes
- Encrypt Media:** Yes
- Override Codecs:** PCMU x G729 x
- Outside Line Prefix:** (empty field)
- E164 Number Format:** E164 without +

At the bottom, a message states: 'The following SBCs are assigned to this service: 20.185.148.172:10951, 52.250.50.231:11208'. There are 'Delete' and 'Save' buttons at the bottom of the form.

## 5 Additional help or support

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

Web: [www.educronix.com](http://www.educronix.com)

Email: [support@educronix.com](mailto: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.

