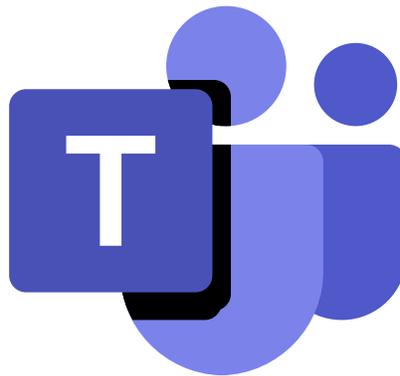




Setting up Ingate's SIParator[®] / Firewall[®]

For



Microsoft Teams

For Ingate SIParators using software release 6.3.3 or later

Table of Contents

Table of Contents	2
1 Minimum Requirements.....	4
1.1 SIParator Version	4
1.2 Ingate Licensing.....	4
1.3 Office Tenant Account	4
1.4 Domain ownership	4
1.5 FQDN/Public IP for the SBC.....	4
1.6 Public Trusted certificate.	4
1.7 Firewall ports and IP addresses properly configured.....	4
1.8 Office 365 infrastructure prerequisites.....	5
1.8.1 Pair your SBC with the Direct Routing Service (DRS)	5
1.8.2 Configure specific users for DRS	6
2 SIParator configuration.....	7
2.1 Topology with SIParator in the DMZ, IPPBX on LAN and ITSP on WAN.....	7
2.1.1 Requirements	7
2.1.2 SBC Domain	8
2.1.3 Deploy the Baltimore Certificate	9
Import the certificate under Basic Configuration → Certificates → CA Certificate	9
2.1.4 SIParator Network configuration.....	10
2.1.5 SIParator SIP Encryption configuration.....	13
2.1.6 Configure SIP Signaling	18
2.1.7 Configure Media Encryption	19
2.1.8 Configure Media Transcoding.....	21
2.1.9 Other Media related configuration	22
2.1.10 Interoperability features	23
2.1.11 ITSP SIP trunk Configuration	23
2.1.12 Dial Plan	26
2.2 Additional considerations.....	28
3 Troubleshooting.....	29

3.1 You lack mTLS29

4 *Additional help or support*30

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
```

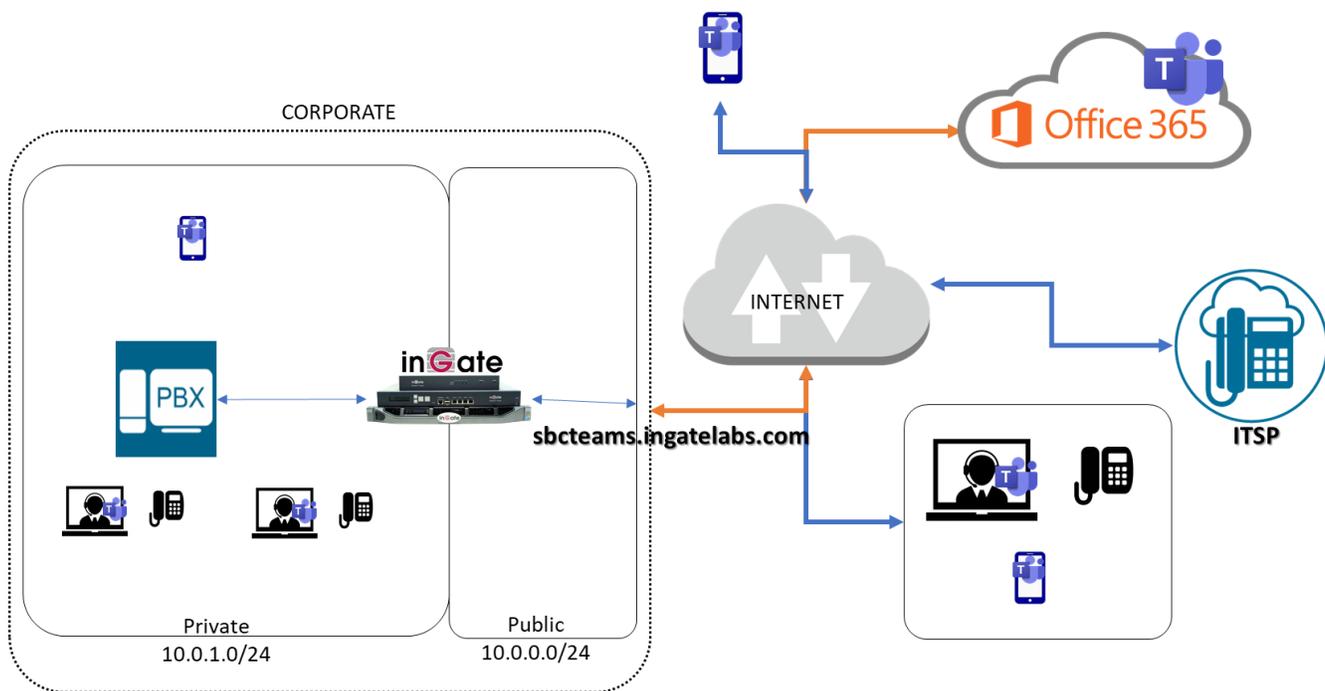
To verify:

```
# Get-CsOnlineUser -Identity " john@mycompany.com " | fl RegistrarPool  
  
RegistrarPool : sippoolC024A05.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@sbcteams.ingatelabs.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:

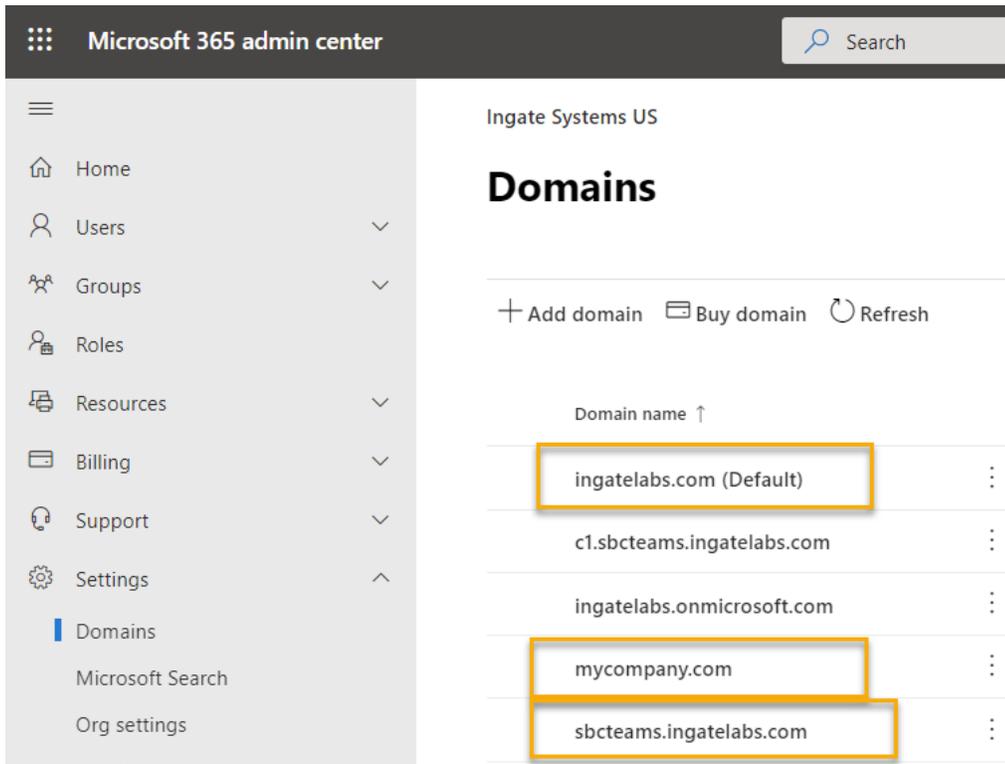
<anyname>.tenant.com, where tenant.com is your domain.

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:

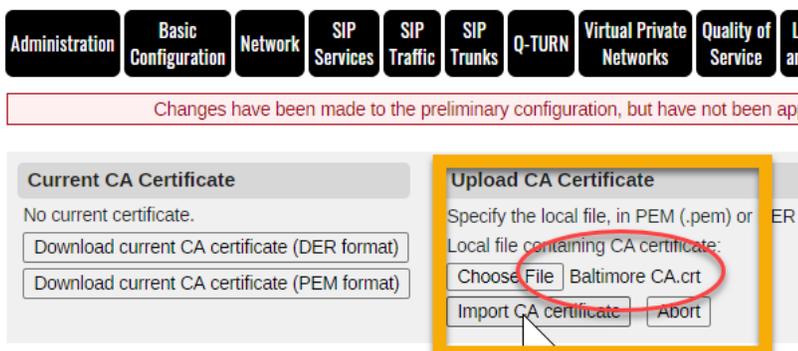


For the purpose of this document we use

sbcteams.ingatelabs.com → 34.195.120.56

2.1.3 Deploy the Baltimore Certificate

Import the certificate under Basic Configuration → Certificates → CA Certificate



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

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

- Certificate imported:
 - Key type: RSA
 - Subject: /C=IE/O=Baltimore/OU=CyberTrust/CN=Baltimore CyberTrust Root
 - Issuer: /C=IE/O=Baltimore/OU=CyberTrust/CN=Baltimore CyberTrust Root
 - Serial Number: 33554617
 - MDS Fingerprint: AC:B6:94:A5:9C:17:E0:D7:91:52:98:B1:97:06:A6:E4
 - SHA1 Fingerprint: D4DE 20D0 5E66 FC53 FE1A 5088 2C78 D828 52CA E474
 - Valid from: 2000-05-12 18:46:00 to 2025-05-12 23:59:00 GMT.
 - Subject Key ID: E5:9D:59:30:82:47:58:CC:AC:FA:08:54:36:86:7B:3A:B5:04:4D:F0

Basic Configuration Access Control RADIUS SNMP Dynamic DNS Update Certificates TLS Settings SIP Parator Type

Private Certificates (help)

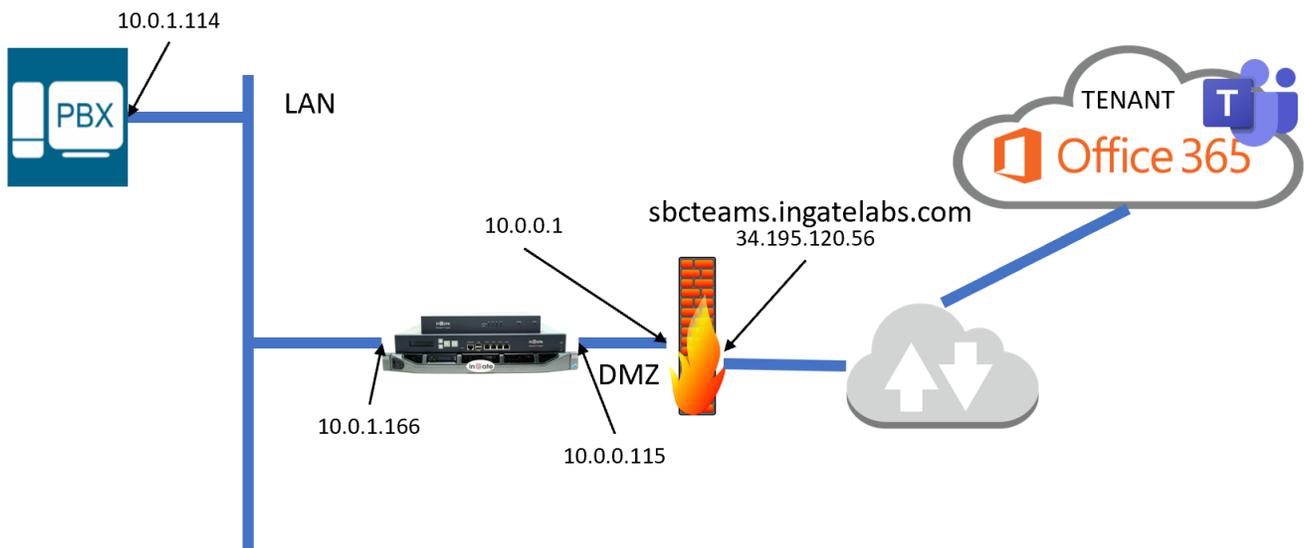
Name	Certificate	Information	Delete Row
httpsconfig	Create New Import View/Download	Key type: RSA Subject: /CN=B041-E7D1-C2B5-DA19-8F1A-5F9D Issuer: /CN=B041-E7D1-C2B5-DA19-8F1A-5F9D MDS Fingerprint: 9E:D4:C5:4E:34:70:90:49:AC:4F:E7:F5:0C:5A:B0:AC SHA1 Fingerprint: 89AC 430C 2E47 A2D9 CE2E 3FEB 7C4D A56F 32D8 4C18 Valid from: 2020-08-25 02:27:41 Valid to: 2021-08-25 02:27:41 Subject Key ID: DC:54:4F:4D:BC:C0:8D:6A:C6:77:3D:68:07:EC:44:F1:E2:E6:7B:43 Authority Key ID: DC:54:4F:4D:BC:C0:8D:6A:C6:77:3D:68:07:EC:44:F1:E2:E6:7B:43	<input type="checkbox"/>

Add new rows 1 rows.

CA Certificates (help)

Name	CA Certificate	CA CRL	Information	Delete Row
Baltimore CA	Change/View	Change/View	Key type: RSA Subject: /C=IE/O=Baltimore/OU=CyberTrust/CN=Baltimore CyberTrust Root Issuer: /C=IE/O=Baltimore/OU=CyberTrust/CN=Baltimore CyberTrust Root MDS Fingerprint: AC:B6:94:A5:9C:17:E0:D7:91:52:98:B1:97:06:A6:E4 SHA1 Fingerprint: D4DE 20D0 5E66 FC53 FE1A 5088 2C78 D828 52CA E474 Valid from: 2000-05-12 18:46:00 Valid to: 2025-05-12 23:59:00 Subject Key ID: E5:9D:59:30:82:47:58:CC:AC:FA:08:54:36:86:7B:3A:B5:04:4D:F0	<input type="checkbox"/>

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:

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

Interface Overview

General

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

Directly Connected Networks (Help)

Name	Address Type	DNS Name or IP Address	IP Address	Netmask / Bits	Network Address	Broadcast Address	Interface or Tunnel	VLAN Id	VLAN Name
outside	Static	10.0.0.115	10.0.0.115	24	10.0.0.0	10.0.0.255	outside (eth0)		
inside	Static	10.0.1.166	10.0.1.166	24	10.0.1.0	10.0.1.255	inside (eth1)		

Add new rows 1 rows.

Static Routing (Help)

Routed Network				Router		Interface or Tunnel	Delete Row
DNS Name or Network Address	Network Address	Netmask / Bits	Dynamic	DNS Name or IP Address	IP Address		
default	default			10.0.0.1	10.0.0.1	outside (eth0)	<input type="checkbox"/>

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

Networks and Computers							
Name	Subgroup	Lower Limit		Upper Limit (for IP ranges)		Interface/ VLAN	Delete Row
		IP Range	IP Range	IP Range	IP Range		
+ ITSP	-						<input type="checkbox"/>
	-						<input type="checkbox"/>
	-						<input type="checkbox"/>
	-						<input type="checkbox"/>
	-						<input type="checkbox"/>
	-						<input type="checkbox"/>
+ LAN	-						<input type="checkbox"/>
+ Loop	-						<input type="checkbox"/>
+ Offices	-						<input type="checkbox"/>
+ PBX	-						<input type="checkbox"/>
	-						<input type="checkbox"/>
	-						<input type="checkbox"/>
+ SIP	ITSP						<input type="checkbox"/>
	LAN						<input type="checkbox"/>
	Offices						<input type="checkbox"/>
	PBX						<input type="checkbox"/>
	Sip-all.pstnhub.microsoft.com						<input type="checkbox"/>
+ SIParator Prox	-						<input type="checkbox"/>
+ Sip-all.pstnhub	-	52.112.0.1	52.112.0.1	52.115.255.254	52.115.255.254	outside (eth0 untagged)	<input type="checkbox"/>
	-	52.120.0.1	52.120.0.1	52.123.255.254	52.123.255.254	outside (eth0 untagged)	<input type="checkbox"/>
+ Teams	Sip-all.pstnhub.microsoft.com					-	<input type="checkbox"/>
	Teams DoD and GCC					-	<input type="checkbox"/>
	Teams Media					-	<input type="checkbox"/>
+ Teams DoD an	-	52.127.64.0	52.127.64.0	52.127.71.255	52.127.71.255	outside (eth0 untagged)	<input type="checkbox"/>
	-	52.127.88.0	52.127.88.0	52.127.95.255	52.127.95.255	outside (eth0 untagged)	<input type="checkbox"/>
+ Teams Media	-	52.112.0.0	52.112.0.0	52.115.255.255	52.115.255.255	outside (eth0 untagged)	<input type="checkbox"/>
	-	52.120.0.0	52.120.0.0	52.123.255.255	52.123.255.255	outside (eth0 untagged)	<input type="checkbox"/>
	-	52.127.64.0	52.127.64.0	52.127.71.255	52.127.71.255	outside (eth0 untagged)	<input type="checkbox"/>
	-	52.127.88.0	52.127.88.0	52.127.95.255	52.127.95.255	outside (eth0 untagged)	<input type="checkbox"/>
+ WAN	-						<input type="checkbox"/>
+ ixnx	-						<input type="checkbox"/>

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:

The screenshot shows the Ingate GUI navigation menu with 'Basic Configuration' selected. Below the menu, a message states: 'Changes have been made to the preliminary configuration, but have not been applied.' A warning message reads: 'This page contains an error.' The 'Certificates' tab is active in the sub-menu. The 'Private Certificates' section is displayed with a table header: Name, Certificate, Information, and Delete Row. The table contains one row with the text 'No certificate exists'. Below the table, a red box highlights the 'Name' input field (containing 'No value given.'), the 'Create New' button, the 'Import' button, and the 'Download' button. The text 'No current certificate' is visible to the right of the buttons.

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

Create Certificate or Certificate Request

Fill in the certificate data for "" 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

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.

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.

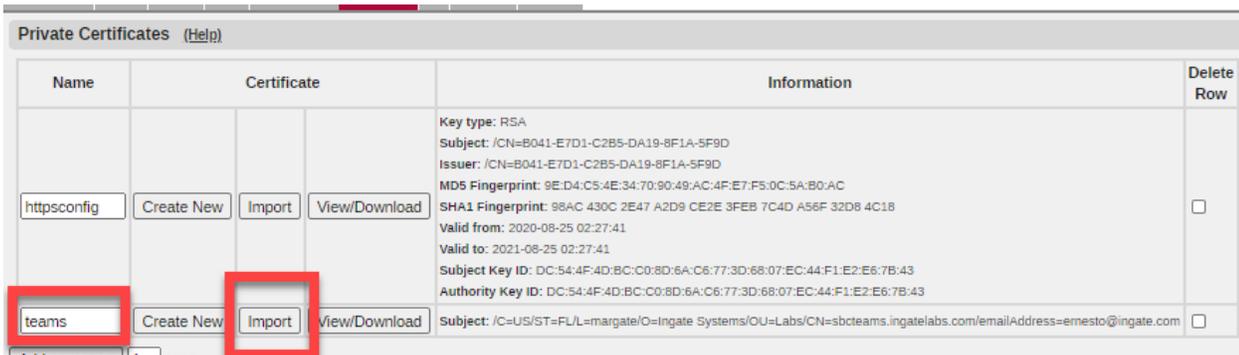
Once you obtain the signed certificate, you'll get more than one file, sometimes in a chain including their CA public half. It might look something like this:

Name	Date modified	Type	Size
sbcteams_ingatelabs_com.ca-bundle	11/19/2019 11:31 AM	CA-BUNDLE File	6 KB
sbcteams_ingatelabs_com	11/19/2019 11:31 AM	Security Certificate	3 KB
sbcteams_ingatelabs_com	11/19/2019 11:31 AM	PKCS #7 Certificates	8 KB

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:

Basic Configuration | Access Control | RADIUS | SNMP | Dynamic DNS Update | **Certificates** | TLS | Advanced Settings | SIParator Type

Private Certificates (Help)

Name	Certificate		Information
httpsconfig	Create New	Import	View/Download
teams	Create New	Import	View/Download

Add new rows | 1 rows

CA Certificates (Help)

Name	CA Certificate	CA CRL	Information	Delete Row
Baltimore CA	Change/View	Change/View	Key type: RSA Subject: /C=IE/O=Baltimore/OU=CyberTrust/CN=Baltimore CyberTrust Root Issuer: /C=IE/O=Baltimore/OU=CyberTrust/CN=Baltimore CyberTrust Root MD5 Fingerprint: AC:B6:94:A5:9C:17:E0:D7:91:52:9B:B1:97:06:A6:E4 SHA1 Fingerprint: D4DE 20D0 5E66 FC53 FE1A 5088 2C78 DB28 52CA E474 Valid from: 2000-05-12 18:46:00 Valid to: 2025-05-12 23:59:00 Subject Key ID: E5:9D:59:30:82:47:58:CC:AC:FA:08:54:36:86:7B:3A:B5:04:4D:F0	<input type="checkbox"/>
Bundle CA	No value given. Change/View	Change/View	No current certificate	<input type="checkbox"/>

Add new rows | 1 rows

Save | Undo

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

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

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

Current CA Certificate

No current certificate.

Download current CA certificate (DER format)

Download current CA certificate (PEM format)

Upload CA Certificate

Specify the local file, in PEM (.pem) or DER (.cer) format, containing the CA certificate.

Local file containing CA certificate:

Choose File | sbcteams_in...m.ca-bundle

Import CA certificate | Abort

Page generated for 'admin' 2020-08-29 12:43:06 -0400

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:

Name	CA Certificate	CA CRL	Information	Delete R
Baltimore CA	Change/View	Change/View	Key type: RSA Subject: /C=IE/O=Baltimore/OU=CyberTrust/CN=Baltimore CyberTrust Root Issuer: /C=IE/O=Baltimore/OU=CyberTrust/CN=Baltimore CyberTrust Root MD5 Fingerprint: AC:86:94:A5:9C:17:E0:D7:91:52:9B:B1:97:06:A6:E4 SHA1 Fingerprint: D4DE 20D0 5E66 FC53 FE1A 5088 2C78 D828 52CA E474 Valid from: 2000-05-12 18:46:00 Valid to: 2025-05-12 23:59:00 Subject Key ID: E5:9D:59:30:82:47:58:CC:AC:FA:08:54:36:86:7B:3A:B5:04:4D:F0	<input type="checkbox"/>
Bundle CA	Change/View	Change/View	Key type: rsa Subject: /C=GB/ST=Greater Manchester/L=Salford/O=Sectigo Limited/CN=Sectigo RSA Domain Validation Secure Server CA Issuer: /C=US/ST=New Jersey/L=Jersey City/O=The USERTRUST Network/CN=USERTrust RSA Certification Authority MD5 Fingerprint: AD:A8:5C:4D:F0:31:FB:92:99:F7:1A:DA:7E:18:F6:13 SHA1 Fingerprint: 33E4 E808 0720 4C2B 6182 A3A1 4B59 1ACD 25B5 F0DB Valid from: 2018-11-02 00:00:00 Valid to: 2030-12-31 23:59:59 Subject Key ID: 8D:8C:5E:C4:54:AD:8A:E1:77:E9:9B:F9:9B:05:E1:B8:01:8D:61:E1 Authority Key ID: 53:79:BF:5A:AA:2B:4A:CF:54:80:E1:D8:9B:C0:9D:F2:B2:03:66:C8	<input type="checkbox"/>

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

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

Signaling Encryption [\(Help\)](#)

Enable signaling encryption
 Disable signaling encryption

TLS Connections On Different IP Addresses [\(Help\)](#)

IP Address	Own Certificate	Use CN FQDN	Require Client Cert	TLS	Delete Row
outside (10.0.0.115) ▼	sbcteams.ingatelabs.com ▼	Yes ▼	Yes ▼	TLSv1.x ▼	<input type="checkbox"/>

Add new rows rows.

Making TLS Connections [\(Help\)](#)

Default own certificate: sbcteams.ingatelabs.com ▼ Use TLS: TLSv1.x ▼

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.

TLS CA Certificates (Help)

CA	Delete Row
Bundle CA	<input type="checkbox"/>
Baltimore CA	<input type="checkbox"/>

Add new rows rows.

Check Server Domain Match (Help)
Check if the server domain matches the certificate:
 Yes No

Allow Wildcard in Server Certificates (Help)
Allow Wildcard in Server Certificates:
 Yes No

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).

Administration Basic Configuration Network Rules and Relays **SIP Services** SIP Traffic SIP Trunks Q-TURN Failo

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

SIP Module (Help)
 Enable SIP module
 Disable SIP module

SIP Signaling Access Control (Help)
Specify the networks and computers from which the firewall accepts SIP Signaling.
-

SIP Signaling Ports (Help)

Active	Port	Transport	Intercept	Comment	Delete Row
Yes	5060	UDP and TCP	Yes	Standard SIP port	<input type="checkbox"/>
Yes	5061	TLS	Yes	Standard TLS port	<input type="checkbox"/>

Add new rows rows.

SIP Media Port Range (Help)
Ports: -

Public IP Address for NATed firewall (Help)
DNS Name or IP Address IP Address

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**.

SIP Servers To Monitor (Help)

Server	Port	Transport	Delete Row
sip.pstnhub.mi		TLS ▼	<input type="checkbox"/>
sip2.pstnhub.n		TLS ▼	<input type="checkbox"/>
sip3.pstnhub.n		TLS ▼	<input type="checkbox"/>
teams.pstn.twi		- ▼	<input type="checkbox"/>
10.0.1.114		- ▼	<input type="checkbox"/>

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.twi... 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.

Public IP Address for NATed firewall (Help)

DNS Name or IP Address	IP Address
sbcteams.ingatelabs.com	34.195.120.56

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:

inGate SBC

Administration Basic Configuration Network Rules and Relays **SIP Services**

Basic Settings Signaling Encryption **Media Encryption** Media Transcoding Interoperability

Media Encryption (Help)

Enable media encryption

Disable media encryption

Enable **Media Encryption**

Crypto Suite Groups (Help)

Name	Suite
+ Any (transcodi	Cleartext (no encryption) SRTP sdesc. (AES-CM 128, SHA1 32) SRTP sdesc. (AES-CM 128, SHA1 80)
+ Cleartext	Cleartext (no encryption)
+ Encrypted (tra	SRTP sdesc. (AES-CM 128, SHA1 32) SRTP sdesc. (AES-CM 128, SHA1 80)
+ SRTP	SRTP sdesc. (AES-CM 128, SHA1 32) SRTP sdesc. (AES-CM 128, SHA1 80)
TEAMS	SRTP sdesc. (AES-CM 128, SHA1 80)

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:

SIP Media Encryption Policy (Help)

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

Add new rows | 1 | rows.

Default Encryption Policy (Help)

Suite requirements:
 Cleartext
 Allow transcoding:
 Yes No

Require TLS (Help)

Require TLS for all cryptos but cleartext
 Do not require TLS

RTP Profile (Help)

Prefer RTP/SAVP (sdescriptions)
 Prefer RTP/AVP (cleartext and legacy encryptions)
 Prefer RTP/AVP (together with sdescriptions)

Multi Profile (Help)

Enable Multi Profile
 Disable Multi Profile

DTLS-SRTP (Help)

Certificate:
 -
 DTLS to use:
 DTLSv1.x
 Add the client's IP to the cookie: Yes No
 Ignore invalid dates in the client's certificate: Yes No

Keep Established Crypto Within a Dialog (Help)

Keep established crypto within a dialog: Yes No

Add Cryptos in the B2BUA (Help)

Add cryptos in the B2BUA: Yes No

Force Media Encryption (Help)

Force media encryption: Yes No

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

Media Transcoding (Help)

Enable media transcoding
 Disable media transcoding

Rules (Help)

No.	Destination	Transport	Codecs	Options	Delete
1	teams	TLS	TEAMS	ICE	<input type="checkbox"/>
2	PBX	UDP	PLAIN	-	<input type="checkbox"/>
3	ITSP	UDP	PLAIN	-	<input type="checkbox"/>

Add new rows: 1 rows

Codecs (Help)

Name	No.	Codec	Parameters	Delete Row
+	1	PCMU	-	<input type="checkbox"/>
+	2	PCMA	-	<input type="checkbox"/>
+	3	OPUS	-	<input type="checkbox"/>
+	4	SILK-WB	-	<input type="checkbox"/>
+	5	SILK-NB	-	<input type="checkbox"/>
+	6	SILK-MB	-	<input type="checkbox"/>
+	7	SILK-SWB	-	<input type="checkbox"/>
+	8	G729A	-	<input type="checkbox"/>
+	9	G729B	-	<input type="checkbox"/>

Codec Parameters (Help)

Name	Parameters	Delete Row
+	1	<input type="checkbox"/>

Add new rows: 1 rows

Options (Help)

Name	Perform	Value	Delete Row
+	ICE	Yes	<input type="checkbox"/>
	RTCP-MUX	Yes	<input type="checkbox"/>
	SSRC	Yes	<input type="checkbox"/>

Add new rows: 1 groups with 1 rows per group.

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

The screenshot displays the 'Sessions and Media' configuration page. The 'Media Proxy' section is highlighted with a red box and contains the following settings:

- Enable Media Proxy
- Disable Media Proxy
- Always use the Media Proxy:
 - Yes
 - No

The 'Media Configuration' section is also highlighted with a red box and contains the following settings:

- 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:
- Allowed amount of media streams per SIP session:
- Support forked media streams:
 - Yes
 - No
- Always Relay Media (Help):
 - Always relay media: Yes No

Other visible settings in the 'Session Configuration' section include:

- Session timer: seconds
- Allowed amount of concurrent sessions (leave blank for no limit):
- Timeout for SIP over TCP/TLS: seconds
- Timeout for one-way media streams:
- Timeout for RTP streams:
- Timeout for RTCP streams:
- Tear down media streams at RTP/RTCP timeouts:
 - Yes
 - No

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

No.	From Network	Action	Delete Row
1	SIP	Process all	<input type="checkbox"/>
2	LAN	Process all	<input type="checkbox"/>
3	sip-all.pstnhub.microsoft.com	Process all	<input type="checkbox"/>
5	ITSP	Process all	<input type="checkbox"/>

Default Policy For SIP Request

Process all
 Local only
 Reject all

Preloaded Route Rules

Default Policy For Preloaded Routes

Reject
 Authenticate
 Remove
 Allow

Policy for Signaling and Media on different Networks

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.

2.1.10 Interoperability features

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

Under SIP Services → Interoperability:

Strip ICE Attributes (Help)

Keep ICE attributes in SDPs
 Strip ICE attributes in SDPs

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.

SIP Trunk 1 (Help)

Enable SIP Trunk
 Disable SIP Trunk

SIP Trunking Service (Help)

Use parameters from other SIP trunk
 Define SIP trunk parameters

Service name: ITSP (Unique descriptive name)
 Service Provider Domain: teams.pstn.twilio.com (FQDN or IP address)
 Restrict to calls from: ITSP (* = No restriction)
 Outbound Proxy: (FQDN or IP address)
 Use alias IP address: (-) (Forces this source address from our side)
 Outbound Gateway: (-) (* = Use Default Gateway)
 Signaling Transport: UDP (* = Automatic)
 Port number:
 From header domain: Provider domain
 Host name in Request-URI of incoming calls: 34.195.120.56 (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: No
 Relay media: Yes
 Exactly one Via header: No
 'gin' registration (RFC 6140): No
 Hide Record-Route: No
 Show only one To tag: No
 SIP 3xx redirection to provider domain: No
 SIP 3xx redirection to caller domain: No
 Route incoming based on: Request-URI (For P-Asserted-Identity)
 Use P-Preferred-Identity: Yes (Instead of P-Asserted-Identity)
 Forward outgoing calls: No
 Send DTMF via SIP INFO: No
 Remove video: No

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.

Main Trunk Line		Outgoing Calls			Authentication		Incoming Calls	
No.	Reg	Display Name	User Name	Identity	User ID	Password	Incoming Trunk Match	Forward to
1	No	ingatelabs	+19547372009	+19547372009		Change Password		

PBX Lines		Outgoing Calls			Authentication		Incoming Calls		
No.	Reg	From PBX Number/User	Display Name	User Name	Identity	User ID	Password	Incoming Trunk Match	Forward to PBX Account
1	No	(*)	\$1	\$1	\$1		Change Password	(+ *)	teams\$1

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”

Setup for the PBX (Help)

Use PBX from other SIP trunk
 Define PBX settings

PBX Name: (Unique descriptive name)

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

PBX Registration SIP Address	Authentication		PBX IP Address	
	User ID	Password	DNS Name or IP Address	IP Address
<input type="text"/>	<input type="text"/>	<input type="text" value="Change Password"/>	<input type="text" value="127.0.0.1"/>	<input type="text" value="127.0.0.1"/>

PBX Network:

Signaling transport: (* = Automatic)

Port number:

Match From Number/User in field:

Common User Name suffix:

To header field:

Forward incoming REFER:

Send DTMF via SIP INFO:

Remote Trunk Group Parameters usage: (* = Don't use TGP)

Local Trunk Group Parameters usage: (* = Don't use TGP)

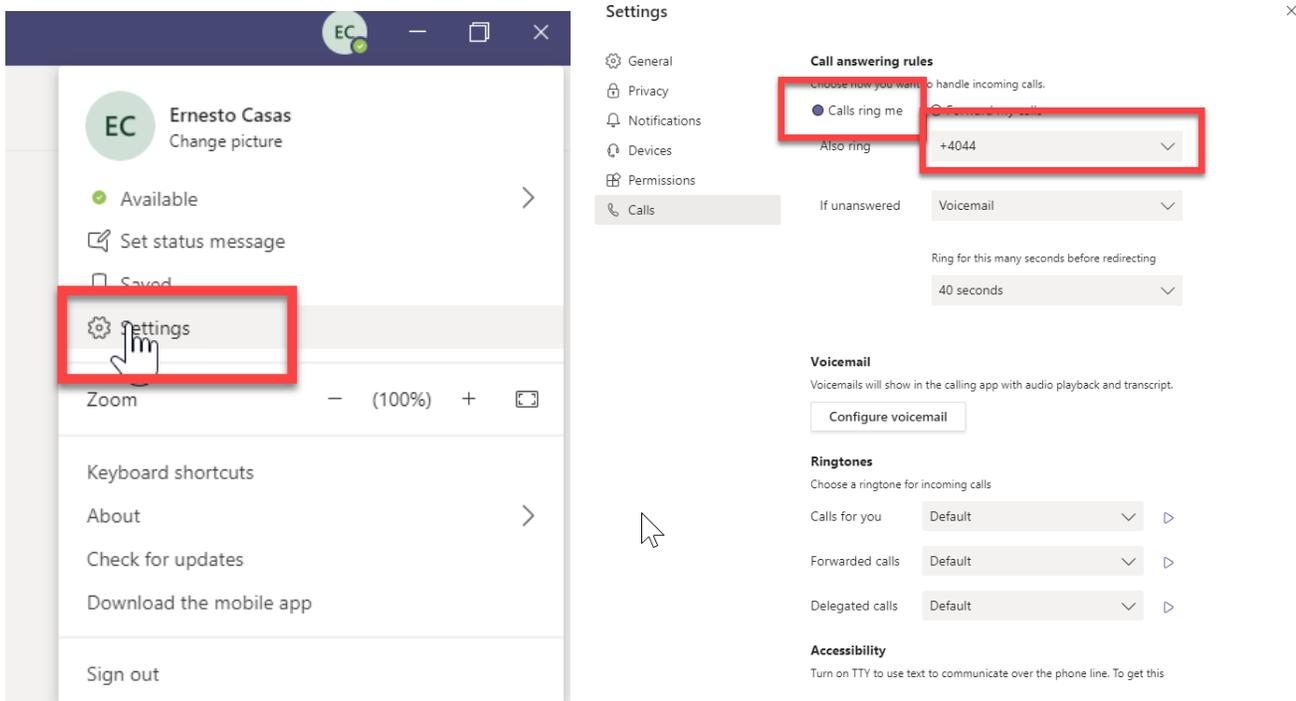
Additional Trunk groups can be used to route calls directly to the IPPBX for DIDs that do not have a configured destination in Teams.

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](#)

The screenshot displays the Ingate SIP Proxy configuration interface. It is divided into four main sections: Matching From Header, Matching Request-URI, Forward To, and Dial Plan.

- Matching From Header:** Contains two rows. The first row, highlighted in purple, has 'From Teams' as the name, '*' for Username and Domain, and 'teams' for the Network. The second row, highlighted in red, has 'Teams SIP OP' as the name and 'sip:[*]+microsoft.com' for the Reg. Expr.
- Matching Request-URI:** Contains three rows. The first row, highlighted in purple, is 'To_PBX'. The second row, highlighted in purple, is 'To_PSTN_USA'. The third row, highlighted in green, is 'To_teams' with the Reg. Expr. 'sip:teams(*)@127.0.0.1'. A purple callout bubble labeled 'Outbound call to PSTN' points to this row.
- Forward To:** Contains three groups of rows. The first group, highlighted in purple, has 'ITSP' as the name and 'SIP Trunk 1: ITSP-Local_loop' as the Trunk. The second group, highlighted in orange, has 'PBX' as the name and 'sip:\$r1@10.0.1' as the Reg. Expr. An orange callout bubble labeled 'Call to PBX' points to this row. The third group, highlighted in green, has 'teams' as the name and three rows for 'sip:\$r1@sip.ps', 'sip:\$r1@sip2.p', and 'sip:\$r1@sip3.p'. A green callout bubble labeled 'Call to Teams' points to this group.
- Dial Plan:** Contains four rows. The first row, highlighted in red, has 'Teams SIP OPTIONS' as the From Header and 'Allow' as the Action. A red callout bubble labeled 'Let OPTIONS be processed by SIP Proxy' points to this row. The second row, highlighted in green, has 'To_teams' as the Request-URI and 'Forward' as the Action. The third row, highlighted in purple, has 'To PSTN_USA' as the Request-URI and 'Forward' as the Action. The fourth row, highlighted in orange, has 'To_PBX' as the Request-URI and 'Forward' as the Action.

4) Dial Plan (Rules are processed 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**” Forward 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@zyzyyx-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.