# **Application Note**



# Connecting Zoom Phone Premise Peering (BYOC & BYOP)

# with Ingate SIParator<sup>®</sup> SBC

Introduction	4
About the Zoom Phone System	4
About Ingate SIParator <sup>®</sup> SBC product family	4
Deployment scenarios	6
Proof of Concept Topology	6
Configuring Zoom Phone System	7
Configuring SIParator <sup>®</sup> SBC	7
Pre-requisites	7
Configuring Inside and Outside Interfaces	8
Other Network related configurations	
Configuring TLS for Zoom	12
Using CSR	12
Using ACME	17
Adding Zoom CA certificates to trust TLS connections	21
Configure NTP Server	22
Setup TLS with Zoom Supported versions	22
Configuring SIP in SIParator <sup>®</sup>	24
Setup TLS signaling	24
Setup SIP Ports	25
Configure Media Encryption	26
Configure SIP Trunking	28
Setting up Zoom-PSTN Trunk Group	29
Setting up PBX-PSTN Trunk Group	
Configure Dial Plan	
Enabling SIP Options for Zoom requests	
Route outbound from Zoom to PSTN	35
Route Outbound from PBX to PSTN	
Route PBX $\leftarrow \rightarrow$ Zoom	
Configuring Transcoding	
Final recommendations and other points of interest	41
Useful Documentation	41
Zoom phone setup and requirements	41
Route Groups (Manage)	42

SIP Groups (Manage)	42
Routing Rules (Manage)	43
Disclaimers	43
Help and Support	43

# Introduction

# About the Zoom Phone System

Zoom Phone is a cloud phone system natively built for the Zoom platform. Seamless and secure, Zoom Phone streamlines the telecommunications experience with enterprise-class features on a unified platform that includes video conferencing and team chat. It offers centralized management, enabling IT teams to easily provision and manage users, as well as monitor call quality and usage data in the Zoom administrator portal.

Zoom Phone easily flows into other Zoom solutions. Zoom Phone users can make and receive phone calls, move the call to video conferencing without requiring participants to hang up or dial into a separate bridge, share content, and send chat messages from Zoom desktop and mobile apps.

Operating on the globally distributed Zoom cloud platform, Zoom Phone is designed to be easy to use while maximizing voice and video quality. It comes with numerous security features and operates on 256-bit AES-GCM encryption.

Zoom Phone offers a variety of plans tailored to your unique business needs. You can select a pricing plan that lets you pay as you go or select from local phone numbers and domestic calling in 40+ different countries. There are also optional add-on plans available to businesses that have at least one licensed user.

Zoom Phone Premise Peering provides organizations with flexibility and seamless options to migrate their voice workloads to the cloud. This is accomplished by providing two connection types; Premise Peering PSTN and/or Premise Peering PBX (formally referred to as Bring Your Own PBX - BYOP). Zoom Phone Premise Peering PSTN enables organizations to leverage their existing telephony carrier PSTN environment for Zoom Phone connectivity. Using this functionality organizations can connect Zoom Phone with virtually any telephony carrier.

# About Ingate SIParator® SBC product family.

A Session Border Controller is a device that connects to an existing network firewall to seamlessly enable SIP communications (Session Initiation Protocol). While traditional firewalls block SIP traffic – including mission-critical applications like Voice over IP (VoIP) – the Ingate SIParator<sup>®</sup> SBC resolves this problem, working in tandem with your current security solutions.

The Ingate SIParator<sup>®</sup> is a powerful, flexible and cost-effective Enterprise Session Border Controller (E-SBC) for SIP connectivity, security and interoperability, such as connecting PBXs and Unified Communications (UC) solutions to SIP Trunking service providers.

The Ingate Firewall<sup>®</sup>, which is always included in the product, makes the Ingate SIParator an all-in-one appliance for data security as well as session border control.

Ingate's SIParators<sup>®</sup>/Firewalls<sup>®</sup> are available in a range of models:



The SIParator simplifies SIP trunking and makes it easy to connect remote UC end points, aggregate SIP trunks and distribute sessions between sites and service delivery points. It's utilized for Real-Time communications security, SIP interoperability and extensive connectivity. The SIParator<sup>®</sup> is compatible with all existing networks and comes with a standard SIP proxy and a SIP registrar. It has support for NAT and PAT as well as for TLS and SRTP to encrypt both SIP signaling and media, eliminating the security issue most associated with using enterprise VoIP.

The flexible system of add-on licenses allows any enterprise to enhance the SIParator<sup>®</sup>/Firewall<sup>®</sup> solution to meet their needs at any given moment.

With more than 10,000 installations worldwide, the Ingate SIParator<sup>®</sup> comes in a wide range of capacities, and has been used by retail companies, financial institutions, industrial firms, government agencies, call centers and small-to-large enterprises.

# **Deployment scenarios**

# **Proof of Concept Topology**

Interoperability between SIParator<sup>®</sup> SBC and Trunking with te Zoom Phone System has been tested in the following setup.



Figure 1: Deployment Layout

Configuration for SIParator<sup>®</sup> in this document will show how to route PSTN traffic to or from either Zoom Phone system or existing customer PBX. Also will show how to route calls between Zoom Users and PBX users (extensions)

We are assuming SIParator will be sitting behind an existing firewall in a DMZ.

Our SIParator will be setup with 2 network interfaces enabled (it is highly recommended not to use single interface), one will be in the DMZ while the other will be in the internal private LAN where the IP PBX is reachable.

Both, Zoom Phone System and the SIP Trunk Provider are located in the WAN or external network (Internet).

The IP-PBX is located in the Private Network

Zoom Phone System uses TLS signaling while the ITSP and IP-PBX both use SIP over UDP

Zoom Phone System operates with encrypted media (SRTP) while ITSP and IP-PBX both use plain RTP for media.

# Configuring Zoom Phone System

For detailed instructions on how to setup Zoom Phone System, you can refer to Zoom Help Center at

https://support.zoom.us/hc/en-us/articles/360001297663-Getting-started-with-Zoom-Phone-admin-

NOTE: Before you begin configuration: ■ Contact your Zoom Representative to enable SIP groups and set up SIP trunks that are directed toward your SBC for your Zoom Phone account. ■ Make sure you have Zoom Portal admin credentials. Be aware that each customer needs to have a Zoom Phone admin account and all Zoom Phone related configuration is done by the customer and not by the carrier.

# Configuring SIParator<sup>®</sup> SBC

# **Pre-requisites**

For this use case, validation has been done running SIParator<sup>®</sup> release 6.4.1 and the minimum licensing needed must include:

- Number of sip trunk concurrent session. Also known as CCS and must be at least the maximum number of concurrent SIP sessions we want the solution to support assigned to 2 Trunk Groups.
- One trunk Group will be supporting simultaneous calls between PBX and PSTN and the second Trunk will be associated to calls between Zoom and PSTN
- We need also to consider the maximum simultaneous calls between Zoom and PBX but they won't use any Trunk Group.
- This can be obtained with CCS shared among the 3 flows (Zoom-PSTN, PBX-PSTN, Zoom-PBX). In this case you will need:

#### Total CCS Needed = Max CCS Zoom-PSTN + Max CCS PBX-PSTN + Max CCS Zoom-PBX

#### One additional Trunk Group Sharing all CCS (License known as TGS)

If you have any doubts or questions about the best options for licensing, feel free to send your questions to <a href="mailto:support@educronix.com">support@educronix.com</a>

No other licenses are needed to this specific use case. When transcoding is needed, there are no license needed as Transcoding feature is a built in functionality purely based on software.

Make sure you are using one of the SIParator<sup>®</sup> appliances according to your expected workload, or a VM properly dimensioned if you are using Software SIParator<sup>®</sup>

Before initiating the deployment make sure you have:

- A Public IP address to be used exclusively for your SBC. It can be assigned in your firewall and properly routed to the SIParator<sup>®</sup> DMZ ip address.
- Public certificates issued by one of the Zoom supported Cas.

### Configuring IP Network Interfaces

SBC Interfaces will be assigned IP addresses for

- Outside Interface. The one sitting in the DMZ and associated to the public IP address.
- Inside Interface. The one that will be used for Management access to SIParator<sup>®</sup> and also to reach internal SIP resources (i.e. IP-PBX).

SBC, in our case, is connected to the WAN/Internet through a DMZ connection.

In our case all interfaces are dedicated ethernet ports.



# **Configuring Inside and Outside Interfaces**

You can use Zoom provided tables for media and signaling IP's. We will use the tables available by the time this document is being created taken for Zoom Documentation.

For signaling:

ľ	Traffic Type	Protocol	Port	Source	A Record	Destination	Region	
			5041 0	Customer SBC		us01peer01.sc.zoom.us us01peer01.ny.zoom.us us01peer01.dv.zoom.us	162.12.233.59 162.12.232.59 162.12.235.85	North America
					us01peer01.sp.zoom.us us01peer01.qr.zoom.us	64.211.144.247 149.137.69.247	LATAM	
	Cionalina	TCD/TLS			us01peer01.am.zoom.us us01peer01.fr.zoom.us	213.19.144.198 213.244.140.198	EMEA	
	Signaling	Signaling TCP/TLS 5061 Ct	Customer SBC	us01peer01.sy.zoom.us us01peer01.me.zoom.us	103.122.166.248 103.122.167.248	Australia		
			us01peer01.sg.zoom.us 149.137.4 us01peer01.ty.zoom.us 207.226.13		149.137.41.246 207.226.132.198	APAC		
l					us01peer01.hk.zoom.us	209.9.211.198	China	
			us01peer01.os.zoom.us us01peer01.ty.zoom.us	149.137.25.246 207.226.132.198	Japan			

For Media:

Traffic Type	Protocol	Source	<b>Destination Ports</b>	Destination IPs	Region
				162.12.232.0/22	North America
		Customer		64.211.144.0/24 149.137.69.0/24	LATAM
				213.19.144.0/24 213.244.140.0/24	EMEA
Media	Media UDP/SRTP SBC	SBC 20000-64000	103.122.166.0/23	Australia	
			1	149.137.41.0/24 207.226.132.0/24	APAC
			209.9.211.0/24	China	
			207.226.132.0/24 149.137.25.0/24	Japan	

For the purpose of this document we will select only LATAM region as our lab is being deployed for Latin America, however you can use the appropriate sections of the table depending on the region you are located or deploying.

First, we will assign all those IP addresses and address ranges names to be easily used later in the configuration

\dmin	istration Basi Configu	ic ration Network HTTP Service	SIP SIP s Services Traffic Tr	SIP unks Q-TURN Vir	tual Private Networks Service	Logging and Tools About	Log out			
Netwo Com	orks and Default puters Gateways	All s Interfaces VLAN Eth(	) Eth1 Status PPPo	E Tunnels Topolog	у					
Ne	Networks and Computers									
			Lower	Limit	Upper (for IP r	Limit anges)	Interface/VLAN	Delete		
	Name	Subgroup	DNS Name or IP Address	IP Address	DNS Name or IP Address		Interface/VLAN	Row		
•	ZM LATAM	] - 🗸 🗸	64.211.144.0	64.211.144.0	64.211.144.255	64.211.144.255	Outside (eth0 untagged) 🗸			
		- 🗸	149.137.69.0	162.12.232.0	149.137.69.255	162.12.232.255	Outside (eth0 untagged) 🗸	] 🗆		
•	ZS LATAM	] - 🗸	us01peer01.sp.zoc	64.211.144.247		]	Outside (eth0 untagged) 🗸	]		
L,			us01peer01.qr.zoo	149.137.69.247			Outside (eth0 untagged) 🗸			
e	zoom	ZM LATAM 🗸	]	]		]	- •			
		ZS LATAM 🗸	]	]		]	- •			

Notice:

- ZM MEDIA  $\rightarrow$  Zoom Media in LATAM
- ZS LATAM  $\rightarrow$  Zoom Signaling in LATAM
- zoom  $\rightarrow$  aggregated addresses for media and signaling in LATAM

Make sure 2 Interfaces are enabled (Active). In our case we are also assigning a name to each one (inside for eth1 and Outside for eth0)

Administration	Ba: Configu	sic Iration	Netwo	ork	HTT Servi	P ces	S Serv	IP vices	SIF Traff	ic T	SIP runk	g-TI	JRN
Networks and Computers	Defaul Gateway	t ys <b>Inte</b>	All rfaces	VLA	N Et	h0	Eth1	Inter Sta	face tus	PPP	oE T	unnels	Торо
Interface	Overv	iew											
General													
Physical E	Device	Interfa	ice Na	me	Ac	tive	9	MTU	1				
eth0		Outsid	le		Ye	s 🗸	15	500					
eth1		Inside			Ye	s 🗸	1	500					
		_	_			-		_	_				_

Looking at our topology:



In our case,

- DMZ Network: 10.1.0.0/24
- LAN Network: 10.1.1.0/24
- Default Gateway: 10.1.0.1

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	Delete Row
	eth0	Static 🗸	10.1.0.145	10.1.0.145	24	10.1.0.0	10.1.0.255	Outside (eth0) 🗸		-	
	eth1	Static 🗸	10.1.1.83	10.1.1.83	24	10.1.1.0	10.1.1.255	Inside (eth1) 🗸		-	
	Add now rows	rowe									

Static route for the default gateway:

Static Routing (H	static Routing (Help)								
Routed Network				Route	er				
DNS Name or Notwork Address	Network Address	Netmask / Bits	Dynamic	DNS Nam or IP Addr	ne ess	IP Address	Interface or Tunnel	Delete Row	
default	default		- 🗸	10.1.0.1		10.1.0.1	Outside (eth0) 🗸		

# **Other Network related configurations**

Let's assign the DNS server address. In our case we are going to use Google DNS 8.8.8.8

Basic Configuration ccess control RADIUS SIParator: te	etwork SNMP V	HTTP Services Ser Dynamic DNS Update 'ersion of So	SIP vices Traffic Certificates	SIP Trunks	Q-TURN Advanced LS Settings	irtua Net SIF
ccess ontrol RADIUS SIParator: te	SNMP V Cł	Dynamic DNS Update Version of So	Certificates	ACME T	Advanced LS Settings	SIF
SIParator:	V Cl	ersion of Se	oftware SI	Dereter		
SIParator:	C			Paraton	/Firewall	
in: Help) P packets packets packets via et	SI Da SC P C C C	heck for new V Parator/Firew ate of last suc oftware versio <b>'olicy For Pi</b> ) Never reply ) Only reply t Reply to pir	versions of S all: cessful vers n in use: i <b>ng To the</b> to ping o ping to the ng to all IP a	Software ion chec SIParat e same ir ddresses	O Y Not a 6.4.1 tor nterface s	es ( vail
rs <u>(Help)</u>						
vnamic C or • 8.8.8	DNS Na TP Add	ame IP A iress 8.8.	ddress De	lete Rov	N	
	Help) P packets packets via et vnamic or 8.8.8	Help)     P       P packets     P       packets via     P       et     P       vnamic     DNS Na       or IP Add       v     8.8.8.8	Policy For Pi Policy For Pi Never reply Packets Policy For Pi Never reply Packets Policy For Pi Never reply Packets Policy For Pi Reply to pir Packets via et Policy For Pi Reply to pir Packets Policy For Pi Packets Poli	Policy For Ping To the         Policy For Ping To the         Packets       Only reply to ping         Packets       Only reply to ping to the         packets via et       Reply to ping to all IP a         S (Help)       DNS Name         Vnamic       DNS Name         Or IP Address       Delays         S (Help)       8.8.8.8         S (Help)       Reply to ping to all IP a	Help)       Policy For Ping To the SIParat         Packets       Only reply to ping         packets       Only reply to ping to all IP addresse         packets via et       IP Address Delete Row         vnamic       DNS Name         ONS Name       IP Address         J. Lows       8.8.8.8	Policy For Ping To the SIParator         Policy For Ping To the SIParator         Only reply to ping         Only reply to ping to the same interface         packets         packets via et         State         DNS Name         IP Address         Delete Row         State         8.8.8         8.8.8

You can also assign a name to this SIParator. The name will displayed in your browser tags.

Let's also assign an NTP server and setup time for the SIParator<sup>®</sup>. We are assuming to be located in EST time zone.

Administration	Basic Configuration	Network	HTTP Services	SIP Services	SIP Traffic	SIP Trunks	Q-TURN	Virtual Priva Networks	te Quality Servic	of Loggir e and To
Save/Load Configuration	Show Configuration	User Administra	ition Upg	Table rade Look	Date al Time	nd Rest	Licen art Serv	ise Change er Language		
Change T DumontDU Dushanbe ( East (Brazi) East-Indian Easter (Pac Easter) (Da Easter) (Da Easter) (Da Change I Date: 202 Time: 133	ime Zone ( inville (Antarcti Asia) ) a (US) iffic) d (Chile) unada) S) Date and Tir 2-10-24 58:04	(Help) (ca)	Active tim Change ally ( <u>He</u>	e zone: E time zone time zone time zone	astern ( Change Synchron	US) • Date a iize time	and Tin e with NT	ne With NT IP: <ul> <li>Yes</li> </ul> <li>If NTP Is E</li>	P ( <u>Help)</u> ○ No nabled	
Save Un	do Look up	all IP add	lresses a	gain	Dynami - • Add new	c or time	DNS Nar TP Addi .nist.gov	me IP / ress 132 ws.	Address 163.97.6	Delete Row

# Configuring TLS for Zoom

In this section we will enable TLS to setup connectivity with Zoom Phone System.

In order to enable TLS we will need appropriate public certificates. With SIParator there are two ways to acquire, install and maintain TLS certificates.

- Using CSR. Generating the Sign Request from the SIParator, submit it to the Certification Authority to get the signed certificate and intermediate certificates (if needed) and install them in the SIParator<sup>®</sup>.
- Using ACME. Using SIParator built in ACME client and use the appropriate ACME enabled Authority in compliance with Zoom accepted CAs.

## Using CSR

First, we will need to create a CSR (Certificate Signature Request).

Under Basic Configuration  $\rightarrow$  Certificates  $\rightarrow$  Private Certificates, add a new row:

Administration Base Configu	sic Iration Network HTTP SIP SIP Services Services Traffic T	SIP runks Q-TURN Virtual Private Quality of Logging Networks Service and Tools About Log out						
	Changes have been made to the preliminary configuration, but have not been applied.							
This page conta Basic Configuration Control	This page contains an error. Basic Access Dynamic DNS Dynamic DNS Certificates ACME TLS SIParator Onfiguration Control RADIUS SNMP Update Certificates ACME TLS Settings Type							
Private Certifica	tes ( <u>Help)</u>							
Name	Certificate	Information	ACME Domain Delete	Row				
No certificate exist	S.							
No value given.	Create New Import View/Download	No current certificate	· •					

Assign a name and click on "Create New"

Fill the Information requested and make sure the Common Name and SubjectAltName extension DNS points to the SIParator FQDN that resolves on the Public IP address associated to the outside interface:

Create Certificate of	or Certificate Reques	t
Fill in the certificate dat	a for " <b>byoc-cert</b> " below,	then create either a certificate or a certific
After generating a certi	ficate request, and havir	ng it signed by a signing authority, the certi
Expire in (days):	Country code (C):	Organization (O):
* 365	US	Educronix
Common Name (CN):	State/province (ST):	Organizational Unit (OU):
* byoc.edx-labs.c	FL	Engineering
Email address	Locality/town (L):	
ernesto@educr	Weston	
SubjectAltName Ex	tension	
Enter the alternative na	ames that you want to ac	ld to a certificate or a
separation.	ipie values carrise adde	a by using comma
Email:		
Dris: byoc.edx-labs.	com	
IP:		

Notice Expire in (days) and Common Name (CN) are mandatory fields.

All remaining fields can be left on default values.

Click on "Create an X.509 certificate request"

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): 2048 🗸
Signature algorithm: SHA-256 V
ACME
Use the ACME protocol for this X.509 certificate O Yes  No
If you generate several certificates with identical data you should make sure they have different Serial number:
* 2
Fields marked with "*" are mandatory.
Create a self-signed X.509 certificate Create an X.509 certificate request Abort

#### Certificate request will show like this:



Apply changes

Administration	Basic Configuration	Network	HT Serv	TP vices S	SIP ervices
	Char	nges have	beer	n made	e to the p
Save/Load Configuration	Show Configuration	User Administra	ition	Upgrad	Table Look
Test Run	and Apply	Conf <u>(He</u>	<u>elp)</u>		Show I
Duration of	limited test n	node:			🔘 On e
30	seconds				○ On t
Apply con	figuration				

Go back to the certificate and Click on "View/Download"

Administration	Bas Configu	ic ration	letwork	HTTP Services	SIP Services Tr	SIP SI affic Tru	P iks	Q-TURN VI	irtual Private Networks	Quality of Service	Logging and Tools	About	Log out					
Basic Configuration	Access Control	RADIUS	SNMP	Dynamic DM Update	IS Certifica	tes ACME	TLS	Advanced Settings	SIParator Type									
Private Co	ertificat	es <u>(He</u>	elp)															
Name	•			Certificat	е							Informa	tion					
byoc-cert		Create	New	Import	View/Dow	nload	ubjec ubjec	t: /C=US/ST tAltName: [	T=FL/L=West DNS:byoc.ed	n/O=Educro -labs.com	nix/OU=En(	gineering/C	N=byoc.e	dx-labs.co	im/emai	IAddress=	ernesto@e	ducronix.cor

Download certificate either in PEM or DER format. It will depend on the CA you'll use to sign it which better fits. We will use PEM for our example.

С	urrent Private Certificate for "byoc-cert"
Cu	rrent certificate request:
	<ul> <li>Subject: /C=US/ST=FL/L=Weston/0=Educronix/OU=Engineering/CN=byoc.edx-labs.com/emailAddress=ernesto@educronix.com</li> <li>SubjectAltName: DNS:byoc.edx-labs.com</li> </ul>
	Download certificate/certificate request (DER format)
	Download certificate/certificate request (PEM format)
_	
R	eturn to certificate page

#### Downloaded file should look like this:



Use it to request the signed certificate from the Certification Authority you have selected.

Once signed they will provide you with a set of files, usually 2:

- Signed Certificate
- Intermediary Bundle Certificates.

Similar to this:

☑ 🗟 byoc_edx-labs_com.ca-bundle	10/21/2022 1:47 PM	CA-BUNDLE File	5 KB
✓ is byoc_edx-labs_com.crt	10/21/2022 1:47 PM	Security Certificate	3 KB

You'll need to load the signed certificate as well as the CA bundle as intermediate certificates. Use the "Import" button to do so:

	Administration	Basi Configu	ic ration	Network	HTTP Services	SIP Services	SIP Traffic	SIP Trunks	Q-TUR	Vi	rtual Private Networks	Quality of Service	Logging and Tools	About	Log out				
l	Basic Configuration	Access Control	RADIUS	SNMP	Dynamic D Update	NS Certi	ficates	ACME T	Adva TLS Sett	nced ings	SIParator Type								
l	Private Ce	ertificat	es <u>(H</u>	<u>elp)</u>															
I	Name	•			Certifica	te							1	nforma	tion				1
l	byoc-cert		Create	New	Import	View/D	ownloa	d Sub	ject: /C=l jectAltNa	JS/ST me: D	=FL/L=Westo DNS:byoc.edx-	n/O=Educror labs.com	nix/OU=Engi	neering/(	CN=byoc.e	dx-labs.com/ema	ilAddress=erne	sto@educronix.co	<b>m</b> [

First import the certificate, save and apply and then load the bundle.



Save and apply the changes again.

You should be able to see the new signed certificate loded similar to this:

I	Basic Configuration	Access Control	RADIUS	SNMP	Dynamic DN Update	S Certificates	ACME	TLS	Advanced Settings	SIParator Type				
l	Private Co	ertificat	tes <u>(He</u>	<u>elp)</u>										
I	Name	•			Certificate							Information		
	byoc-cert		Create	New	Import	View/Downloac	Ke Su Iss Sig SF SF Va Va Su Su Su	ey Typ Ibject Suer: gnatu D5 Fin IA-1 F IA-25 Iid fro Iid to Ibject Ibject	e: RSA :: /CN=byoc. /C=GB/ST=4 ine Algorithm agerprint: E Fingerprint: 6 Fingerprint : 022-10 : 2023-10-11 : AltName: D : Key ID: 28 ty Key ID: 8	edx-labs.co Greater Mar n: sha256V F:CC:59:D3 0-18 00:00:0 3 23:59:59 NS:byoc.ed 64 D	m ichester/L=Salford/O=S /ithRSAEncryption :EB:0C:04:9F:61:32:7E 0 x-labs.com, DNS:www	Sectigo Limited/CN= E:AB:7C:B9:7C:0E v.byoc.edx-labs.com	Sectigo RSA Domain 1 8E:E1:D8 1:8D:61:E1	Validation Secure Server CA C99 D450 8061 0ED9

# Using ACME

Before creating the certificate, we will need to have SIParator<sup>®</sup> ACME feature enabled and properly configured.

Administration	Bas Configu	Basic Configuration		HTTP Services	SIP Services	SIP Traffic	SIP Trunk	s	Q-TURN	Virtual Private Networks	Quality of Service	Loggi and To
Basic Configuration	Access Control	RADIUS	SNMP	Dynamic D Update	NS Certi	ficates	ACME	TLS	Advance Setting	ed SIParator ss Type		
ACME (H	lelp)											
Enable	the ACM	1E proto	ocol									
<ul> <li>Disable</li> </ul>	the ACM	VE proto	ocol					_				

For the purpose of this document, we have selected one Certification Authority supporting ACME protocol that complies with Zoom requirements.

ZeroSSL (<u>https://zerossl.com/</u>) is the one we will use here as their root certificate has a chain of trust included in Zoom recognized certification authorities.

dministration	Bas Configu	ic ration	letwork	HTTP Services	SIP Service	S Tra	IP S ffic Tru	IP nks	Q-TURN	Virtual Privat Networks	te Qual Ser	lity of vice	Loggin and Too	g Is About
		Change	es have	been ma	ide to th	ne prel	iminary	confi	guratior	n, but have n	ot beer	n appli	ied.	
Basic Configuration	Access Control	RADIUS	SNMP	Dynamic I Update	DNS e Cei	rtificat	es ACM	TLS	Advand Settin	ed SIParator gs Type				
ACME (H	<u>elp)</u>													
<ul> <li>Enable t</li> <li>Disable</li> <li>Account</li> </ul>	the ACN the ACN s <u>(Hel</u> f	1E protoc /IE proto ))	col											
Accounts	associa	ted with	the AC	ME proto	col.									
Nar	ne			Contact			Priv	vate K	(ey	EAB Key ID	EA	BHM	IAC Key	/ Delet
ZweroS	SL	mailto:	ernest	o@educro	onix.cor	m	Cre	ate N	ew d	tGH0a110Bt	nê Cl	hange	e Secret	
Add new	rows	1 row	s.					-						

- Assign Name
- Add contact information with the format <u>mailto:xxxxx@yyyy.zzz</u> to provide who will be receiving updates and notifications from the CA.
- Generate a "Private Key" by pressing "Create New"
- Add EAB Key ID and EAB HMAC Key provided by the CA (for ZeroSSL, it can be found in the Developers Section)

Add the service

Services (Help)													
A service that supports the ACME protocol.													
Name	Domain or IP	Directory Path	Trusted CA	Delete Row									
ZeroSSL	acme.zerossl.com	v2/DV90	Bundle 🗸										
Add new rows 1	rows.												

- Assign a Name
- Enter the domain provided by the CA (for ZeroSSL is "acme.zerossl.com")
- Enter Directory path as provided by the CA (for ZeroSSL is "v2/DV90")
- You must have a bundle CA certificate previously loaded containing CA root certificates for your trusted CA's)
- •

Add a Domain name to be used and referred when creating new ACME managed certificates.

Domains (Help)												
Domains that should be available to use with the ACME protocol.												
Name	HTTP-01 Challenge Address	Service	Account	Renewal Interval (%)	Delete Row							
zoom	eth0 (10.1.0.145) 🗸	ZeroSSL 🗸	ZweroSSL 🗸	67								

- Assign a Name
- Select the interface that will be facing the outside (Internet)
- Select the Service and Account (previously created).
- Keep the default value of 67% to establish when the request for renewal will be triggered

Now we are ready to create the Certificate using ACME.

Like in "Using CSR" we will create a Certificate Sign Request, but in this case we will select ACME tag.

Add a new row in Private Certificates and assign a name, click o "Create New":

	Basic Configuration	Access Control	RADIUS	SNMP	Dynamic DM Update	IS Certificates	ACME 1	Advan TLS Settin	ced 1gs	SIParator Type			
	Private Ce	ertifica	tes ( <u>He</u>	<u>lp)</u>									
	Name	e			Certificat	е					Information	1	ACME Doma
Π.	No certifica	te exist	s.										
	byoc.edx-l	abs	Create	New	Import	View/Downloa	d No	current ce	ertific	cate		[	- •
							Kev	Type: RS4		_			_

#### Complete the information here:

Create Certificate or	Certificate Reques	t
Fill in the certificate data	a for " <b>byoc.edx-labs</b> " b	elow, then create either a (
After generating a certifi	cate request, and havir	ng it signed by a signing at
Expire in (davs):	Country code (C):	Organization (O):
* 365	US	Educronix
Common Name (CN):	State/province (ST):	Organizational Unit (OU)
* byoc.edx-labs.c	FL	Engineering
Email address	Locality/town (L):	
ernesto@educr	Weston	
SubjectAltName Ext	ension	
Enter the alternative nar certificate request. Multi separation.	nes that you want to ac ple values can be adde	ld to a certificate or a d by using comma
Email:		
URI:		
DNS: byoc.edx-labs.c	om	
IP:		

Notice:

- Expire and Common name are mandatory fields, however, Expire will be defined by the Certification Authority regardless of the value you enter.
- Common Name and DNS must match the FQDN associated with the SIParator<sup>®</sup> public IP.

ACME
Use the ACME protocol for this X.509 certificate Ves No
If you generate several certificates with identical data you should make sure they have different
Serial number:
* 2
Fields marked with "*" are mandatory.
Create a self-signed X.509 certificate Create an X.509 certificate request Abort
age generated for 'admin' 2022-10-26-08:41:07-0400

- Select "Yes" in the ACME section
- Press on "Create an X.509 certificate request.

This creates a temporary self signed certificate until the CA provides the new signed certificate.

Make sure you associate the ACME domain to this new certificate.

byoc.edx-labs Create New	Import View/Download	Key Type: RSA Subject: /C=US/ST=FL/L=Weston/O=Educronix/OU=Engineering/CN=byoc.edx-labs.com/emailAddress=ernesto@educronix.com Issuer: /C=US/ST=FL/L=Weston/O=Educronix/OU=Engineering/CN=byoc.edx-labs.com/emailAddress=ernesto@educronix.com Signature Algorithm: sha256WithRSAEncryption MD5 Fingerprint: C0:6A:08:1A:89:7C:56:45:1F:47:D8:07:BF:CA:04:A6 SHA-1 Fingerprint: 598:0597 3CD8 4469 3130 9FCB CD25 FDBF EC49 9079 SHA-256 Fingerprint: 548:0597 3CD8 47E5 98CA 7427 DE06 FBE9 56F1 A0BB DEB6 01FC 5079 785F 2247 7155 Valid from: 2022-10-25 21:33:37	zoom 🗸
--------------------------	----------------------	---	--------

#### Save and apply changes

In a few more seconds you'll see the new certificate already signed by the ACME compliant CA of your choice.

s)	Name		Certificate Information		ACME Domain		
	byoc.edx-labs	Create New	Import	View/Download	Key Type: RSA Subject: /CN=byoc.edx-labs.com Issuer: /C=AT/O=ZeroSSL/CN=ZeroSSL/RSA Domain Secure Site CA Signature Algorithm: sha284WithRSAEncryption MD5 Fingerprint: 0B:AC SHA.256 Fingerprint: 0B SHA.256 Fingerprint: 6 Valid from: 2022-10-21 00:00:00 Valid to: 2023-01-19 23:59:59 Subject Key ID: C8: Authority Key ID: C \$;	82 2950 9A1F 4F72 8A7B	zoom 🗸

In the case of ZeroSSL, you can see the certificate and intermediate (trust chain) by selecting "View/Donwload"



Notice USERTrust RSA Certification Authority is included in Zoom accepted CAs.

If you have questions regarding other ACME options feel free to send your inquires to <a href="mailto:support@educronix.com">support@educronix.com</a>

## Adding Zoom CA certificates to trust TLS connections

By the time this document is released, Zoom Certificates are all signed by Digicert. You should add all Digicert root certificates in the CA section of SIParator<sup>®</sup> Basic Configuration.

Here you can just add a bundle that includes DIgicert root certificates. A good source for this bundle can be found here: <a href="https://curl.se/docs/caextract.html">https://curl.se/docs/caextract.html</a>

Or you can download all Digicert needed CA root certificates from Digicert directly here:

https://cacerts.digicert.com/DigiCertGlobalRootCA.crt.pem

https://cacerts.digicert.com/DigiCertGlobalRootG2.crt.pem

https://cacerts.digicert.com/DigiCertGlobalRootG3.crt.pem

In any case, to install any of the previously mentioned Bundle or specific Cas certificates, you can do it here:

Under Basic Configuration  $\rightarrow$  Certificates, in the CA Certificate section:

CA Certificate	s <u>(Help)</u>			
Name	CA Certificate	CA CRL	Information	Delete Row
No value given. Bundle	No value given Change/View	Change/View	No current certificate	0
Add new rows	1 rows.			

- Assign a name (Bundle in our case)
- Click on CA Certificate "Change/View"



- Select the file you download in the previous section
- Click on "Import CA certificate"

In the case of the Bundle, you will see about 142 certificates loaded under the same name.



Apply and Save your changes.

# **Configure NTP Server**

To have SIParator<sup>®</sup> well synchronized with your time zone, make the right configuration here:



# Setup TLS with Zoom Supported versions

It is known that Zoom supports only TLS v1.2. In this section we will create a TLS profile that includes only TLSv1.2 and it will be used in TLS setup for SIP later in this document.

Iministration Confi	asic guration	HTTP SIP Services Services	SIP Traffic Trunks Q-TURN Virtu No	ual Private Quality of Logging etworks Service and Tools	Abou
Basic Acces	s di radius snmp	lynamic DNS Update Certi	ficates ACME <b>TLS</b> Advanced S Settings	SIParator Type	
TLS Settings	(Help)				
Name	Protocols	Ciphers	Diffie-Hellman Group	ECDH Curve	Delet Rov
DTLSv1.x	DTLSv1.x	✓ HIGH ✓	MODP2048 (Group 14) 🗸	NIST P-256 (secp256r1) 🗸	
SSLv3.0	SSLv3.0	✓ HIGH ✓	MODP2048 (Group 14) 🗸	NIST P-256 (secp256r1) 🗸	
TLSv1.2	TLSv1.2	✓ HIGH ✓	MODP2048 (Group 14) 🗸	NIST P-256 (secp256r1) 🗸	
TLSv1.x	TLSv1.x	✓ HIGH ✓	MODP2048 (Group 14) 🗸	NIST P-256 (secp256r1) 🗸	
TLSv1.x & SSL	TLSv1.x & SSLv3	3.0 V HIGH V	MODP2048 (Group 14) 🗸	NIST P-256 (secp256r1) V	
Name	Protocol	Delete Row			
+ DTLSv1.x	DTLSv1.0 V	0			
	DTLSv1.2 V		4		
+ SSLv3.0	SSLv3.0 🗸	0	•		
+ TLSv1.2	TLSv1.2 V				
+ TLSv1.x	TLSv1.1 V				
	TLSv1.2 ¥				
+ TLSv1.x & S	SL SSLv3.0 🗸				
	TLSv1.0 V				
	TLSv1.1 V				
	TLSv1.2 V				
Add new rows	1 groups with 1	rows per grou	ıp.		

- Add a new entry in the Protocols section which includes only TLSv1.2, we named it "TLSv1.2
- Save, and then add a new entry in TLS Settings table as shown in the picture above. We also named it "TLSv1.2"

# **Configuring SIP in SIParator®**

Now we will setup all signaling related configuration for SIP.

#### Setup TLS signaling

Administration	Basic Configuration	Network Se	HTTP ervices	SIP Services	SIP Traffic	SIP Trunks	Q-TURN	Virtual Privat Networks	e Quality o Service
Basic Signa Settings Encryp	ling Media tion Encrypti	Media on Transcodi	ng Inter	roperabilit	Sessio y Me	ons and edia	Remote S Connectiv	SIP VolP vity Survival	
Signaling E	Encryption	(Help)							
Enable si	gnaling encry	ption							
<ul> <li>Disable si</li> </ul>	gnaling encr	yption							
TLS Conn	ections On	Different I	P Addi	resses	(Help)				
IP Add	Iress	Own Certif	icate	Use CN EQDN	Requi Clier	ire ht	TL	s	Delete Row
eth0 (10.1.	0.145) 🗸 🚺	yoc.edx-lab	s 🗸	No 🗸	Yes 🔊	<ul> <li>TL</li> </ul>	Sv1.2	~	
Add new to		ws.	_		_	_			
Making TL	S Connect	ions <u>(Help</u>	)						
Delault own	centificate.	USE ILS.			1				
zoombyoc_	1year 🗸	TLSv1.2		~					
TLS CA C	ertificates	(Help)							
CA	Delete R	ow							
Bundle	•								
Digicert 2	•								
Digicert 3	•								
Digicert A	<ul> <li>✓</li> <li>□</li> </ul>								
Add new ro	ws 1 ro	WS.							

- Add a new raw under "TLS Connections on Different IP Addresses"
- Associate your outside interface (eth0) to receive and generate TLS traffic
- Select the certificate to be presented by SIParator<sup>®</sup> (The one we created before).
- Disable "Use CN FQDN" and enable "Require Client Cert" to be compliant with Zoom requirement of support MTLS.
- Select the recently created profile for TLSv1.2
- Use the same certificate as the default for any other TLS connection
- Add the Trusted CA root certificates based on what you configured before. Just remember that for Zoom we will only need the 3 Digicert CAs.

You will also leave the next two setting in "No" as shown here:



#### Setup SIP Ports

Now we will need to associate ports to be used for SIP (UPD/TCP and/or TLS)

Go under SIP Services  $\rightarrow$  Basic Settings



- Make sure SIP Module is enabled
- By default, SIP Signaling port 5060 for UDP and TCP is already enabled and "Allow from" enables access from any network. We can later restrict this for only sources we trust for UDP or TCP.
- Activate port 5061 for TLS, enable Intercept a restrict for traffic only coming from the Zoom zone you have defined before (in our case we created a network name "ZS LATAM" and we will restrict or allow only from those IP's.
- As our SIParator<sup>®</sup> is sitting in a DMZ, the public IP is NATed and we need to write down the public IP address as indicated.

We at this point also want to monitor Zoom SIP proxy IP addresses. In our case we know LATAM uses the ones indicated below. SIParator<sup>®</sup> will monitor those IP's by sending periodically SIP OPTIONS.

SIP Servers To Monitor (Help)				
Server	Port	Transport	Delete Row	
us01peer01.qr.:		TLS 🗸		
us01peer01.sp.		TLS 🗸		
Add new rows	L rows.			

We are monitoring then:

- us01peer01.qr.zoom.us (Latam México)
- us01peer01.sp.zoom.us (Latam Sao Paulo)

As Zoom uses port 5061, we don't need to explicitly indicate any port to monitor (5061 is the default for TLS). We just need to select TLS.

#### **Configure Media Encryption**

Zoom requires, besides TLS as signaling encryption, the media to be also encrypted (SRTP)

To configure Media Encryption, make sure it is enabled:



Then we will create a Crypto Suite Group specifically for Zoom

Name	Suite	Delete Ro
+ Any (transcoda	Cleartext (no encryption)	
	SRTP sdesc. (AES-CM 128, SHA1 32) 🗸	
	SRTP sdesc. (AES-CM 128, SHA1 80) 🗸	
+ Cleartext	Cleartext (no encryption)	
+ DTLS-SRTP	DTLS-SRTP	
Encrypted (tran	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) 🗸	
	SRTP sdesc. (AES-f8 128, SHA1 80) 🗸	
+ SRTP Zoom	SRTP sdesc. (AES-CM 256, SHA1 80) 🗸	
	SRTP sdesc. (AES-CM 128, SHA1 32) 🗸	
	SRTP sdesc. (AES-CM 128, SHA1 80) 🗸	

- Add one row with 3 sub-rows
- Select each sub-row associated to the suites shown in the picture

Add a Media Encryption Policy:

SIP Media	a Encryption Policy	/ <u>(Help)</u>			
No.	Network	Transport	Suite Requirements	Allow Transcoding	Delete Row
1	zoom 🗸	TLS 🗸	SRTP Zoom	Yes 🗸	
Add power					

- Add a new row
- Select the aggregated network named "zoom"
- Select TLS for transport protocol
- Associate the recently created suite named "SRTP Zoom"
- Enable "Allow Transcoding"

Define a default encryption policy for anything else:

21 2 · · ·	<u>teip)</u>
Suite requirements: Al	low transcoding:
Cleartext 🗸 🧿	Yes O No

- Select "Cleartext" as the default policy (Cleartext means "No Encryption")
- Allow Transcoding

Set the remaining parameters as shown:

Require TLS (Help)
Require TLS for all cryptos but cleartext
O Do not require TLS
RTP Profile (Help)
<ul> <li>Prefer RTP/SAVP (sdescriptions)</li> </ul>
Prefer RTP/AVP (cleartext and legacy encryptions)
O Prefer RTP/AVP (together with sdescriptions)
Multi Profile (Help)
O Enable Multi Profile
Disable Multi Profile
DTLS-SRTP (Help)
DTLS:
DTLSv1.x V
Add the client's IP to the cookie: <ul> <li>Yes</li> <li>No</li> </ul>
Ignore invalid dates in the client's certificate: O Yes
Keep Established Crypto Within a Dialog (Help)
Keep established crypto within a dialog: O Yes 🖲 No
Add Cryptos in the B2BUA (Help)
Add cryptos in the B2BUA: • Yes O No
Force Media Encryption (Help)
Force media encryption: 🔿 Yes 🖲 No

# Configure SIP Trunking

Let's understand how SIP flows looks like in our case:



### Setting up Zoom-PSTN Trunk Group

In our case we are using Twilio SIP Trunking Service for demonstration purposes.

First, we need to add a Network Name for Twilio provided IP addresses. They can be found in Twilio Website (<u>https://www.twilio.com/docs/sip-trunking/ip-addresses</u>). We will include only North America Virginia IP's as the SIParator is hosted in AWS Virginia Region.

		Lower	Limit	Upper (for IP I	Limit anges)	
Name	Subgroup	DNS Name or IP Address	IP Address	DNS Name or IP Address	IP Address	Interface/VLAN
			_		_	
Twilio	Twilio Media 🗸				]	•
	Twilio Signaling 🗸					-
Twilio Media	- •	34.203.250.0	34.203.250.0	34.203.251.255	34.203.251.255	Outside (eth0 untagge
	- 🗸	54.172.60.0	54.172.60.0	54.172.61.255	54.172.61.255	Outside (eth0 untagge
		E4 172 60 0	54.172.60.0	54.172.60.3	54.172.60.3	Outside (eth0 untagge
Twilio Signalinç	- •	54.172.00.0	_			
Twilio Signalinç	- •	54.172.00.0				
Twilio Signaling	· •	54.172.00.0				

Let's setup the Trunk Group

First, we will enable a new Trunk Group by enabling from the pull-down options:



Click on "Goto SIP Trunk page" and Enable the Trunk Group

We are using Twilio Elastic SIP Trunk Service and have as assigned FQDN: zoompeering.pstn.twilio.com

SIP Trunking Service (Help)		
○ Use parameters from other SIP trunk		
Define SIP trunk parameters		
Service name:	Twilio Trunk	(Unique descriptive name)
Service Provider Domain:	zoompeering.pstn.twilio.com	(FQDN or IP address)
Restrict to calls from:	Twilio 🗸	('-' = 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:	- 🗸	('-' = Automatic)
Port number:		
From header domain:	Provider domain 🗸	
Host name in Request-URI of incoming calls:	3.217.32.189	(Trunk ID - Domain name)

- Assign a name to the trunk group
- Use the provided Proxy FQDN as the Service Provider Domain.
- As our SIParator<sup>®</sup> is behind a firewall (DMZ) we will need to enter the public IP in the Host Name in Request-URI.

Configure the following option in the trunk and leave everything else with default values:

I	Host name in Request-URI of incoming calls:	3.217.32.189	
	Relay media:	Yes 🗸	
	Service Provider domain is trusted:	Yes 🗸	

Now we will setup the Matching rules to route inbound DID's designated for Zoom users or auto attendant:

No. Dog	Outgoi	ng Calls		Auth	nentication	Incomin	g Calls	
No. Reg	Display Name	User Name	Identity	User ID	Password	Incoming Trunk Match	Forward to	
1 No 🗸		+19548668899	+19548668899		Change Password			
DV Linoc (Holp)								
PBX Lines ( <u>Help)</u>								
PBX Lines <u>(Help)</u>	Outgo	ng Calls		Auth	nentication	Incomi	ng Calls	Delete Dev
PBX Lines <u>(Help)</u> No. Reg From PBX Numl:	Outgoi per/User Display Name	ng Calls User Name	Identity	Auth User ID	nentication Password	Incomi Incoming Trunk Match	ng Calls Forward to PBX Account	Delete Row
No. Reg 1 No V	Outgoi ber/User Display Name	ng Calls User Name	Identity	Auth User ID	Password Change Password	Incomi Incoming Trunk Match (\+19548668899)	ng Calls Forward to PBX Account \$1	Delete Row

If you have more than one DID, you can keep adding rows to the PBX Lines table and match additional DID's. You can also use regular Expression for Matching.

The DID (E164 format) setup in the Main Trunk Line (User and Identity) will be used for Caller ID purposes in outbound calls. In our case we are using the DID assigned to the Auto attendant in Zoom.

	company Number: Set					
Add	Import Export					
Q Se	earch			Number Type (All)	<ul> <li>Assigned to (All)</li> </ul>	Status (All)
ssign	SMS/MMS Disable SMS/MMS	Area 🛊	Number Type	Capability	Assigned To	Number State
	(954) 852-8529	Fort Lauderdale, Florida, United States	Toll Number	Incoming & Outgoing	Main Auto Receptionist (Auto Receptionist) Ext. 801	Normal
		Fort Loudordolo, Florido		Incoming 8 Outpoint	Ernesto Casas	Normal
)	(954) 852-8530	United States	Toll Number	incoming & Outgoing	Ext. 800	

Now we are configuring the connection from this trunk group to Zoom.

If zoom destination are no more than two IP addresses or FQDNs then we can use the PBX section for the trunk assigning both to the domain field separated by ",".

Setup for the PBX (Help)					
<ul> <li>Use PBX from other SIP trunk</li> <li>Define PBX settings</li> </ul>					
PBX Name: Zoom Peer		(Unique descriptive	name)		
Use alias IP address: 🚭		(Forces this source	address from our side)		
	Auth	nentication	PBX IP Add	Iress	
PBX Registration SIP Address	User ID	Password	DNS Name or IP Address	IP Address	PBX Domain Name
		Change Password			us01peer01.qr.zoom.us,us01peer
(At least one of PBX Registration, IP addre	ss or Domain Nar	ne is required to locate the	PBX)		
PBX Network:	ZS LATAM	~			
Signaling transport:	TLS 🗸		('-' = Automatic)		
Port number:					
Match From Number/User in field:	From URI	~			
Common User Name suffix:			]		
To header field:	Same as Re	quest-URI 🗸			
Forward incoming REFER:	No 🗸				
Send DTMF via SIP INFO:	No 🗸				
Remote Trunk Group Parameters usag	e: -		✓ ('-' = Don't use T	GP)	
Local Trunk Group Parameters usage:	-		✓ ('-' = Don't use T	GP)	

• Select "Define PBX Settings

- Assign a Name
- In "PBX Domain Name" enter the 2 known Zoom FQDNs (for their LATAM region in our example)

I	Traffic Type	Protocol	Port	Source	A Record	Destination	Region	
					us01peer01.sc.zoom.us us01peer01.ny.zoom.us us01peer01.dv.zoom.us	162.12.233.59 162.12.232.59 162.12.235.85	North America	
l					us01peer01.sp.zoom.us us01peer01.qr.zoom.us	64.211.144.247 149.137.69.247	LATAM	
	Circulium	TODALS	50/1	CustomersPC	us01peer01.am.zoom.us us01peer01.fr.zoom.us	213.19.144.198 213.244.140.198	EMEA	
l	Signaling		5061	Customer SBC	us01peer01.sy.zoom.us us01peer01.me.zoom.us	103.122.166.248 103.122.167.248	Australia	
l					us01peer01.sg.zoom.us us01peer01.ty.zoom.us	149.137.41.246 207.226.132.198	APAC	
L					us01peer01.hk.zoom.us	209.9.211.198	China	
					us01peer01.os.zoom.us us01peer01.ty.zoom.us	149.137.25.246 207.226.132.198	Japan	

#### us01peer01.qr.zoom.us, us01peer01.sp.zoom.us

- Select the Network (ZS LATAM), created previously in Network → Networks and Computers
- Select TLS Signaling.
- Leave the remaining fields with default values.

#### Setting up PBX-PSTN Trunk Group

In this section we assume the ITSP will provide also service for Trunking with DID's associated to the PBX; in this way you can use a single SIParator<sup>®</sup> to manage PSTN traffic for Zoom users as well as your existing PBX.

We will need to add a new Trunk Group page



Enable Tunk Group and select "Use parameters from other SIP Trunk". This way we will use the same Trunk we already configured in the previous section.

O Disable SIP Trunk         SIP Trunking Service (telp)         ● Use parameters from other SIP trunk         ○ Define SIP trunk parameters         Witio Trunk ∨         Main Trunk Line (telp)         No.       Reg         Display Name       User Name         User ID       Password         I No ∨       +19548667575         PBX Lines       telp)         No.       Reg         Outgoing Calls       Authentication         Incoming Trunk Match       Forward to PBX         PBX Lines       Display Name       User Name         Identity       User ID       Password         Incoming Trunk Match       Forward to PBX         2       No.       Change Password       Incoming Trunk Match	Enab	ole SIP Ti	runk							
SIP Trunking Service (Help)       Use parameters from other SIP trunk         Define SIP trunk parameters       Define SIP trunk v         Main Trunk Line (Help)       Main Trunk Line (Help)         No. Reg       Outgoine Calls         Display Name       User Name         User ID       Password         Incoming Trunk Match       Forward to         PBX Lines       (Help)         No. Reg       Outgoing Calls         From PBX Number/User       Display Name         User Name       Identity         User ID       Password         Incoming Calls       Incoming Calls         PBX Lines       Outgoing Calls         Yow       Display Name       User Name         Identity       User ID       Password         Incoming Trunk Match       Forward to PBX         2       No       Change Password       (H10548667575)	) Disal	ble SIP T	runk							
● Use parameters from other SIP trunk         ○ Define SIP trunk parameters         SIP Trunk Parameters         Main Trunk Line (Help)         Main Trunk Line (Help)         No.       Reg         Outgoin Calls       Authentication         Incoming Trunk Match         Forward to         PBX Lines       User Name         User Name       User Name         User Name       User ID         PBX Lines       Help)         No.       Reg         Outgoing Calls       Authentication         Incoming Trunk Match       Forward to         PBX Lines       User Name         User Name       User ID         PBX Lines       Outgoing Calls         No.       Reg         From PBX Number/User       Display Name         User Name       Identity         User ID       Password         Incoming Trunk Match       Forward to PBX         Uno       Change Password       (+19548667575)	SIP T	runking	Service (Help)							
O Define SIP trunk parameters SIP Trunk Parameters Main Trunk Line (telp) No. Reg Outgoin Calls Display Name User Name User Name User Name Identity User ID Password Incoming Trunk Match Forward to PBX Lines (telp) No. Reg From PBX Number/User Display Name User Name User Name User Name Identity User ID Password Incoming Calls Change Password Incoming Calls Change Password Incoming Calls Change Password Incoming Calls Incoming Trunk Match Forward to PBX [2] No ▼	O Us	e parame	eters from other SIP trunk							
SIP Trunk Parameters Twilio Trunk           SIP Trunk Parameters Twilio Trunk V         Main Trunk Line (Helg)         No.       Reg       Outgoin Calls       Authentication       Incoming Calls         No.       Reg       Outgoin Calls       Authentication       Incoming Trunk Match       Forward to Forward to Password         PBX Lines       Helgy       Outgoin Calls       Authentication       Incoming Calls         No.       Reg       Outgoin Calls       Authentication       Incoming Calls         PBX Lines       Helgy       Outgoin Calls       Authentication       Incoming Trunk Match       Forward to PBX         No.       Reg       Outgoin Calls       Authentication       Incoming Trunk Match       Forward to PBX         No.       Reg       Outgoin Calls       Authentication       Incoming Trunk Match       Forward to PBX         Vo.       Reg       Outgoin Calls       Authentication       Incoming Trunk Match       Forward to PBX         Quice       Display Name       User Name       Identity       User ID       Password       Incoming Trunk Match       Forward to PBX         Quice       Outgoin Calls       Change Password       Incoming Trunk Match       Forward to PBX	O De	fine SIP t	trunk parameters							
Main Trunk Line (Help)         Authentication       Incoming Calls         No.       Reg       Outgoin Calls       Authentication       Incoming Trunk Match       Forward to         1       No.       Image: Stress of the stress of th	SIP Tr	runk Para	ameters Twilio Trunk 🗸							
Main Trunk Line (tells)         No.       Reg       Outgoing Calls       Authentication       Incoming Calls         1       No. v       Display Name       User Name       Identity       User ID       Password       Incoming Trunk Match       Forward to         1       No. v       Image Calls       Image Calls       Change Password       Image Calls       Image Calls         PBX Lines       Outgoing Calls       Authentication       Incoming Calls         No.       Reg       Outgoing Calls       Authentication       Incoming Calls         PBX Lines       User Name       Identity       User ID       Password       Incoming Calls         No.       Reg       Outgoing Calls       Authentication       Incoming Calls       Incoming Trunk Match       Forward to PBX         2       Nov       Image Calls       Image Calls       Image Calls       Image Calls       Image Calls										
No.     Reg     Outgoin Calls     Auth-rication     Incoming Trunk Match     Forward to       1     No     Image: Strate Str	Main	n Trunk	Line ( <u>Help)</u>							
No.     Reg     Display Name     User Name     Identity     User ID     Password     Incoming Trunk Match     Forward to       1     No.     Image: State of the s				Outgoir	g Calls		Auth	entication	Incomin	g Calls
I     No     +19548667575     Change Password       PBX Lines       Outgoing Calls     Authentication       No.     Reg     Outgoing Calls     Authentication     Incoming Calls       No.     Reg     Outgoing Calls     Authentication     Incoming Trunk Match     Forward to PBX       2     No     Colspan="4">Change Password	NO.	Reg		Display Name	User Name	Identity	User ID	Password	Incoming Trunk Match	Forward to
PBX Lines     Outgoing Calls     Authenticion     Incoming Calls       No.     Reg     Outgoing Calls     Authenticion     Incoming Calls       No.     Reg     Display Name     User Name     Identity     User ID     Password     Incoming Trunk Match     Forward to PBX       2     No     Image: Colspan="5">Change Password     Image: Colspan="5">Image: Colspan="5" Colspan="5">Image: Colspan="5" C	1	No 🗸			+19548667575	+19548667575		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         2       No v										
No.         Reg         Incoming Calls         Authentication         Incoming Calls           From PBX Number/User         Display Name         User Name         Identity         User ID         Password         Incoming Trunk Match         Forward to PBX           2         No         Image: Call state	PBX	Lines	(Help)							
No.     Reg     From PBX Number/User     Display Name     User Name     Identity     User ID     Password     Incoming Trunk Match     Forward to PBX       2     No	Na	Der		Outgoir	ng Calls		Auth	entication	Incom	ing Calls
2 No V Change Password (+1(9548667575) \$1	NO.	Reg	From PBX Number/User	Display Name	User Name	Identity	User ID	Password	Incoming Trunk Match	Forward to PBX Acco
	2	No 🗸						Change Password	\+1(9548667575)	\$1

- Enable The Trunk
- Use parameters from other SIP trunk and chose Twilio Trunk (configured in the previous section)
- Wi will use a different DID and will add it to the outgoing User Name and Identity for Caller ID purposes.
- For incoming call will match the DID assigned to PBX Trunking. If you have mora tan one DID you can keep adding rows in the PBX Lines.

Now we will setup the PBX connectivity

O Use PBX from other SIP trunk					
Define PBX settings					
PBX Name: Educronix PBX		(Unique descriptive	name)		
Use alias IP address: 🚭		(Forces this source	address from our side)		
	Auth	entication	PBX IP Add	ress	
PBX Registration SIP Address	User ID	Password	DNS Name or IP Address	IP Address	PBX Domain Name
		Change Password			10.1.1.172
(At least one of PBX Registration, IP addre	ess or Domain Nam	ne is required to locate the	PBX)	L.	
PBX Network:	PBX Educror	nix 🗸			
Signaling transport:	· •		('-' = Automatic)		
Port number:					
	From URI	~			
Match From Number/User in field:					
Match From Number/User in field: Common User Name suffix:			]		
Match From Number/User in field: Common User Name suffix: To header field:	Same as Rec	quest-URI 🗸	]		
Match From Number/User in field: Common User Name suffix: To header field: Forward incoming REFER:	Same as Rec	quest-URI 🗸	]		
Match From Number/User in field: Common User Name suffix: To header field: Forward incoming REFER: Send DTMF via SIP INFO:	Same as Red No 🗸	quest-URI 🗸	]		
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 usag	Same as Red No 🗸 No 🗸 Je: -	quest-URI ✔	✓ ('.' = Don't use T	GP)	

- Select "Define PBX Settings"
- Assign a name to the PBX
- In PBX Domain enter the IP address of your PBX (In our case 10.1.1.172)

Select the Network name previously added into Network → Networks and computers. If you
haven't done yet, see the following example:

ŀ	dministration	Basic Configurati	Network	HTTP Services	SIP Services	SIP Traffic	SIP Trunks Q-TU	RN Virtu Ne	ial Private etworks	Quality of Service	Logging and Tools Abou	ut Log out	
	Networks and Computers	Default Gateways I	All nterfaces V	'LAN EthO	Inter Eth1 Sta	rface itus PPF	PoE Tunnels	Topology					
L	Networks	and Com	puters										
l	Nam	10	Subar			Lower	Limit		(1	Upper Lir for IP rang	nit Jes)	Interface/VLAN	Delet
L	Ivan	le	Subgro	λαμ	DNS N	lame Idross	IP Addr	ess	DNS Na	ume trocc	IP Address	Interface/VLAN	Row
	+ PBX Ec	tucronix	-	~	10.1.1.172	2	] 10.1.1.172	2				Inside (eth1 untagged)	•

• Leave the remaining fields with the default values.

# **Configure Dial Plan**

Using Dial Plan we will be able to route outbound traffic, traffic between Zoom and PBX and also enable the SIParator<sup>®</sup> to respond to Zoom Options requests.

First you'll need to enable Dial Plan.



### **Enabling SIP Options for Zoom requests**

We will need to detect Options requests landing in the outside interface. SP Options send requests to the external public IP similar to this:



We will use a regular expression to match the r-uri to an IP address, like this:

sip:@?3.217.32.189

Under Dial Plan, lets match Request URI to the expression:

Matching Requ	iest-URI ( <u>Help)</u>						
Nama			Or This	Delete Deur			
ivame	Prefix	Head	Tail	Min. Tail	Domain	Reg Expr	Delete Row
Options			- 🗸			sip:@?3.217.32.189	

- Assign a name to the rule
- Enter the regular expression.

Under Dial Plan  $\rightarrow$  Dial Plan, add the rule to "allow" Options.

ľ	Dial Plan	<u>(Help)</u>									
L	No	From Hoador	Request-	Action	Eonward To	Add	Prefix	ENUM Poot	Time	Commont	Dele
	NO.	FIOIII Headel	URI	Action	Forward 10	Forward	ENUM	ENOW ROOT	Class	Comment	Ro
L	1	- 🗸	Options 🗸	Allow 🗸	- ~			- 🗸	- 🗸		
L	Add new ro	ws 1 rows	3.				-				

We will use then the Dial Plan for 3 main purposes:

- Route outbound traffic to PSTN from Zoom
- Route outbound traffic to PSTN from PBX
- Route intra-network calls between Zoom Users and PBX Users

#### Route outbound from Zoom to PSTN

To detect/match traffic coming from Zoom we will add a rule in the match From header section

Administra	tion Con	Basic figuration	Network Serv	TP vices Servic	SIP Traffic	SIP Trunks	Q-TURN	Virtual Priv Network	vate Qua s Se	ality of rvice	Logging and Tools	About	Log out
Methods	Filtering	Local Registrar	Authentication	Accounts \$	Call STIR Contro	Dial Plan	Routing	Accounting	Time Classes	IDS/IPS	Test Agent	Status	
Use D	ial Plan	(Help)	Emerge	ncy Numb	er <u>(Help)</u>								
<ul> <li>On</li> <li>Off</li> <li>Fall</li> </ul>	back		911										
Match	ning Fro	om Head	er <u>(Help)</u>										
	Name	Use	Use This ername	3 Domain		Or Reg E	This Expr	Tra	nsport		Netwo	ork	Delete Row
From Add n	Zoom ew rows	*	// *					TLS	`	ZSI	.ATAM	~	

- Add a row in Matching From Header
- Assign a name to the rule
- Use "\*" wildcard for Username and Domain.
- Select the transport protocol to be detected (TLS)

Select the network from which the traffic will be coming from (Zoom Signaling sources)

Add a Request-URI rule to match traffic received for further forward to PSTN

Matching Requ	est-URI (Help)						
Namo			Use This			Or This	Doloto Pr
Name	Prefix	Head	Tail	Min. Tail	Domain	Reg Expr	Delete Rt
Options			- 🗸			sip:@?3.217.32.189	
To PSTN			- 🗸			sip:\+?([0-9]{10,})@3.21	

- Add a new row in "Matching Request-URI"
- Assign a name to the new rule
- Match SIP requests to an E164 number sip:\+([0-9]{10,0}@<SIParator public ip address>

Now we will define destination to PSTN Trunk (Forward to) using the Zoon-PSTN Trunk Group

For	rward To <u>(Help</u>	)								
	Namo	No	Use This	Or	This		Or This	Or This	Lico Alias ID	Doloto Dow
lle	Name	NO.	Account	<b>Replacement Domain</b>	Port	Transport	Reg Expr	типк	USE Allas IP	Delete Row
Ð	To ITSP Zoom	1	- 🗸			• •		SIP Trunk 1: Twilio Trunk;Zoom Peer 🗸	- 🗸	
Add	i new rows 1	grou	ps with 1	rows per group.						

- Add a new row in "Forward to" table
- Assign a name to the rule
- Select Trunk 1 as the destination (The one we created with the ISTP for Zoom DIDs)

Next let's define the actual Dial Plan rule to send outbound traffic to PSTN coming from Zoom.

Ľ	Dial Plan	<u>(Help)</u>									
L	No	From Hoodor	Request-	Action	Forward To		Add Prefix		Time	Commont	Delete
L	NO.	FIUIII Header	URI	Action	Forward To	Forward	ENUM	ENOW ROOL	Class	Comment	Row
L	1	- 🗸	Options 🗸	Allow				- 🗸	- 🗸		
L	2	From Zoom 🗸	To PSTN 🗸	Forward 🗸	To ITSP Zoom 🗸			- •	- 🗸		
	_										

 Build a rule where If From Header matches "From Zoom" and Request-URI matches "To PSTN", the Forward to "To ITSP Zoom"

#### Route Outbound from PBX to PSTN

Now we are ready to add dial plan rules to route outbound to PSTN coming from PBX.

Add a "Forward to" rule pointing to the second trunk we crated to PBX – PSTN connectivity.

F	orward To <u>(Help</u> )	l –							
	Name		Use This	Or	This		Or This	Or This	
	Name	NO.	Account	Replacement Domain	Port	Transport	Reg Expr	Trunk	USE Allas IP
	To ITSP PBX	1	- 🗸			- •		SIP Trunk 2: Twilio Trunk;Educronix PBX 🗸	~
	To ITSP Zoom	1	- 🗸			- 🗸		SIP Trunk 1: Twilio Trunk;Zoom Peer 🗸	- 🗸

- Add a new Row in "Forward to" table.
- Assign a name to the new rule
- Select Trunk 2 (The one we previously created for PSTN connectivity for the PBX)

Add the actual Dial Plan routing rule:

1	Dial Plan	(Help)								
	No	From Header	Request-	Action	Forward To	Add F	Prefix	ENUM Root	Time	Comment
	NO.	riomneauer	URI	Action	roiward io	Forward	ENUM	ENOWINOUT	Class	comment
	1	- 🗸	Options 🗸	Allow	- •			- 🗸	- 🗸	
L	2	From Zoom 🗸	To PSTN 🗸	Forward 🗸	To ITSP Zoom 🗸			- 🗸	- 🗸	
	3	From PBX 🗸	To PSTN 🗸	Forward 🗸	To ITSP PBX 🗸			· •	- 🗸	

- Add a new row to "Dial Plan"
- Match From Header with "From PBX" rule and Request-URI with "To PSTN", and "Forward" to the previously created route named "To ITSP PBX"

Next step will be to add the routing rules needed to move traffic Zoom Users/Extensions  $\leftarrow \rightarrow$  PBX Users/Extensions

## Route PBX ← → Zoom

Here we will detect calls to Zoom extensions by matching to a 3 or 4 digit number arriving to SIParator<sup>®</sup> from the PBX, or matching to a 3 or 4 digit number arriving to SIParator<sup>®</sup> from Zoom.

Name			Use This			Or This	Delete Deu
Name	Prefix	Head	Tail	Min. Tail	Domain	Reg Expr	Delete Rov
Options			- 🗸			sip:@?3\.217\.32\.189	
To PBX extensi			- 🗸			sip:\+?([0-9]{3,4})@3.21	
To PSTN			- 🗸			sip:\+?([0-9]{10,})@3.21	
To Zoom exten:			- •			sip:([0-9]{3,4})@10.1.1.8	

- Add a new row for matching dialing to a PBX extension. This call will arrive to the outside interface to the public IP address of the SIParator<sup>®</sup>.
- Assign a name to the new row.
- Enter the matching string "sip:\+?([0-9]{3,4}@<SIParator public IP>

- Add a new row for matching dialing to a Zoom extension. This call will arrive to the inside interface to the private IP address of the SIParator<sup>®</sup>.
- Assign a name to the new row.
- Enter the matching string "sip:\+?([0-9]{3,4}@<SIParator inside private IP>

Add the "Forward to" destinations for call directly routed to the PBX or to Zoom.

Forward To <u>(Hel</u>	<u>p)</u>									
Nomo	No	Use This	Or	This			Or This	Or This	Lice Alice ID	Delete Ber
Name	NO.	Account	Replacement Domain	Port	Trans	sport	Reg Expr	Trunk	USE Allas IP	Delete Rov
To Cust PBX	1	- 🗸			-	~	sip:\$r1@10.1.1	· •	- 🗸	
+ To ITSP PBX	1	- 🗸			-	~		SIP Trunk 2: Twilio Trunk;Educronix PBX 🗸	- 🗸	
To ITSP Zoom	1	- 🗸			-	~		SIP Trunk 1: Twilio Trunk;Zoom Peer 🔹 🗸	- 🗸	
+ To Zoom	1	- 🗸			•	~	sip:\$r1@us01p	· •	- 1	
	2	- 🗸			-	~	sip:\$r1@us01p	· •	- •	

- Add a new row to define a route to reach the PBX
- Assign a name to the new row
- Use RegExp to define the destination: sip:\$r1@<PBX IP Address>
- Add ";transport=udp;b2buawm" at the end of the expression.
- Add a New row and a sub-row to define the 2 destinations associated to LATAM Zoom Region signaling FQDNs. User Regex to define each one:
  - o *sip:\$r1@us01peer01.qr.zoom.us;transport=tls;b2buawm*
  - sip:\$r1@us01peer01.sp.zoom.us;transport=tls;b2buawm
  - Make sure the "No." has the lowest value for the destination with the highest priority to select. In our example the highest priority corresponds to *sip:\$r1@us01peer01.qr.zoom.us;transport=tls;b2buawm*

Let's now define the rules in the actual dial plan

μ	Dial Plan	(Help)									
L	No	From Header	Poquest LIPI	Action	Forward To	Add	Prefix	ENUM Root	Time	Comment	De
L	NO.	rionineauer	Request-oni	Action	roiward io	Forward	ENUM	ENOMINOUT	Class	comment	R
L	1	· •	Options 🗸	Allow	· •			- 🖌	- 🗸		С
	2	From Zoom 🗸	To PBX extension 🖌	Forward 🗸	To Cust PBX 🗸			- 🗸	- 🗸		C
Ľ	3	From Zoom 🗸	To PSTN 🗸	Forward 🗸	To ITSP Zoom 🗸			- 🗸	- 🗸		С
	4	From PBX 🗸	To Zoom extension 🗸	Forward 🗸	To Zoom 🗸			- 🗸	- 🗸		C
ľ	5	From PBX 🗸	To PSTN 🗸	Forward 🗸	To ITSP PBX 🗸			- •	- 🗸		C
L.											

- Add 2 new rows, one to route calls form Zoom to PBX and the second one to route calls from PBX to Zoom.
- When matching From Header to "From Zoom" and Request-URI to "To PBX extension", Forward the call to "To Cust PBX"
- When matching From Header to "From PBX" and Request-URI to "To Zoom extension", Forward the call to "To Zoom"
- Make sure the rules for extension to extension have lower "No" value than the corresponding rule for PSTN (as shown in the previous picture)

# **Configuring Transcoding**

Premises Peering connections, both via the Internet or private circuit options, will prefer the following codecs in the order of preference listed below:

- OPUS
- G.722
- G.711A-law/μ-law
- G.729

SIParator<sup>®</sup> has software-based transcoding built-in with no extra licensing requirement.

You'll need to enable Transcoding:



We will first create the codec groups needed:

Name	No.	Codec	Parameters	Delete Row
Anyother	1	- 🗸	- 🗸	]
Zoom	1	OPUS 🗸	] - 🗸	] 🖸
	2	G722 🗸	- 🗸	] 🖸
	3	PCMU 🗸	- 🗸	] 🖸
	4	PCMA 🗸	- 🗸	] 🖸
	5	G729A 🗸	. 🗸	] 🖸
	6	G729B 🗸	- 🗸	] 🖸
	7	- *	- 🗸	10

- Add 1 row, and 1 additional row with 7 subrows.
- The first row, named Anyother in our example will have no selection in the Codec Column. This means that Any codec is supported in the group.

 Second Row, named Zoom, with have one sub-row per each Zoom supported Codec as mentioned before

Let's associate which codecs are associated to which signaling network:

Rules (Help)												
No.	Destination		Trans	port	Codecs	Options	Del					
1	ZS LATAM	~	TLS	~	Zoom 🗸	- 🗸						
2	Twilio	~	-	~	Anyother 🗸	- 🗸						
3	PBX Educronix	~	-	~	Anyother 🗸	- 🗸						
Add new r	ows 1 rows.	-		-								

- For Zoom Signaling Network, when using TLS transport, associate Zoom codec group.
- For Twilio (ISTP), for any transport, associate "Anyother" codec group.
- Same thing for "PBX Educronix".

Make sure Media Proxy is enabled:



# Final recommendations and other points of interest

# **Useful Documentation**

- <u>SIParator<sup>®</sup> Reference Guide 6.4.1</u>
- How to use Generic Header Manipulation
- <u>Orientation and Installation Ingate Software SIParator® Firewall/SIParator</u>

# Zoom phone setup and requirements

The most important requirement is to have your Zoom account enabled for Zoom phone with BYOC and BYOP features enabled. This can be done by contacting your Zoom Sales rep and find out the commercial requirements to have them enabled.

One you have it enable you'll notice the following fact in your Zoom Account dashboard.

First you'll notice a Phone System Admin section:



## Select Company Info and then Account Settings

There are 4 important sections you need to pay attention to:

	Multiple Sites	Multiple Sites				
	Routing	Multiple Sites Once enabled, your ourrent site will default to your Main Site.				
	Desk Phone					
	Hours	Surface.				
	Call Park	Routing				
	security	BYOC Settings				
	Outbound Caller ID	Configurations for Bring Your Own Carrier (BYOC).				
	Audio Prompt	S Allow Caller Name Delivery				
Templates Caller Name information will be included in the signaling messages for a BYOC (Premises) call						
	Others					
		Route Groups Manage				
		Nouse uroups are composed of one or more Session Border Controllers and assigned to SIP groups to determine the routing behavior for BYOC-P and BYOP-P calls. When a				
		Koute Group is assigned to a Kegion, calls are originated or terminated on the Zoom data centers that are part of that Kegion. Admine can receive email alerts when a SIP trunk status changes.				
		Email Recipients				
		View in Alerts & Notifications				
		SIP Groups Manage				
		Define SIP Groups and series Route Groups to them, so as to route the calls placed by BYOC numbers, or import external contacts for Global Directory. Any outgoing calls from				
		the SIP Groups will be routed to the specific Route Groups.				
Durfue Data and		Partice Pales - Hanne				
		Kouung kules manage				
		not match a defined External Contact, these rules are tested next. If a dialed number does not match any rules, the call will be routed via the PSTN.				

# Route Groups (Manage)

You will be able to see the connection status for both services (BYOC & BYOP)

Route Group								
Last Updated Time: 07:23 PM, Nov 01, 2022								
Q Search by Name Typ								
Display Name 🗘	Session Border Controllers	Туре 💿	Backup Route Group	Provision Status				
ELLC_RG1 Region @ : South America (São Paulo) Mexico and Central America (Queretaro, MX)	Sequential:	BYOP-P						
ELLC_RG1 Region @ : South America (São Paulo) Mexico and Central America (Queretaro, MX)	Sequential: 3.217.32.189:5061 3.217.32.189:5061	BYOC-P						

## SIP Groups (Manage)

You'll need to have at least one SIP Group for BYOC and one for BYOP like this:

SIP Groups							
Add	Add						
Q Se	Q Search by Name						
Delete	Delete						
0	Name	Route Group					
0	Testing Trunk for BYOP 🕕	ELLC_RG1	Edit				
O	BYOC SBC (i) Testing Trunk for BYOC	ELLC_RG1	Edit				
Page Size 15 · Total 2							

#### Routing Rules (Manage)

Here you should have defined your routing rules for calling to PBX extensions (BYOP) or dialing to PSTN via your SBC (BYOC).

Routing Rules							
Rules defined at the site dialed number does not	ules defined at the site level have higher precedence than rules defined at the account level. If a ialed number does not match any rules, the call will be routed via the PSTN.						
Number matching patterns for routing rules must not conflict with DTMF codes. Click here for support.							
Add Routing Rule							
Test Routing Rules @							
Order Edit Order	Rule Name	Number Pattern	Translation	Routing Path	Call Forwarding		
1	To PBX Extension	^(\d{3,4})\$	\$1	Testing Trunk for BYOP	Disabled	Edit	
2	To PSTN via SBC	^\+?(\d{10,}}\$	+\$1	BYOC SBC	Disabled	Edit	

# Disclaimers

SIParator® and Ingate® are Trademarks of Ingate System AB

Zoom<sup>®</sup> and Zoom Phone<sup>®</sup> are trademarks of Zoom Video Communications, Inc.

This documentation is intellectual property of Educronix LLC and is copyright protected

# Help and Support

In case you need additional information, advise or any type of support regarding the content of this document, please contact:

Educronix LLC 1331 St Tropez Cir #601 Weston, FL 33326 +1 954 866 8884 info@educronix.com