

Application Note



ZoomPhone Local Peering (BYOC and BYOP) using Ingate SIParator[®] SBC

Introduction	4
About the Zoom Phone System	4
About Ingate's SIParator® SBC product family.....	4
Deployment scenarios	6
Proof-of-concept topology.....	6
Zoom Phone System Settings.....	7
SIParator® SBC Configuration	7
Prerequisites	7
Configuring internal and external interfaces	8
Other network-related settings	13
Configuring TLS for Zoom.....	14
Use of CSR	14
Using ACME.....	19
Adding Zoom CA certificates to trust TLS connections	22
Configure the NTP server	24
Configuring TLS with Zoom Supported Versions	24
SIP Configuration in SIParator®	26
Configuring TLS Signaling	26
SIP Port Configuration.....	27
Configure media encryption	28
Defining DNS Override to Handle Traffic Distributed to Zoom with Failover or Balancing	30
Configure SIP trunking	31
Configuring the Zoom-PSTN Trunk Group	32
PBX-PSTN Trunk Group Configuration	35
Configure the dial plan.....	37
Enabling SIP Options for Zoom Requests.....	37
Zoom to PSTN Output Path.....	39
PBX to PSTN Output Path.....	41
PBX Route ←→Zoom.....	41
Transcoding settings	43
Final recommendations and other points of interest.....	45
Useful documentation	45
Zoom Phone Settings and Requirements	45

Route Groups (Manage).....	46
SIP Groups (Manage)	46
Routing Rules (Manage).....	47
Declarations	47
Help and support	47

Introduction

About the Zoom Phone System

Zoom Phone is a cloud phone system built natively 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, allowing IT teams to easily provision and manage users, as well as monitor call quality and usage data in the Zoom admin portal.

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

Powered by Zoom's globally distributed cloud platform, Zoom Phone is designed to be easy to use and maximize voice and video quality. It comes with numerous security features and works with AES-GCM 256-bit encryption.

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

Zoom Phone on-premises peering provides organizations with flexibility and seamless options to migrate their voice workloads to the cloud. This is achieved by providing two types of connection; Premise Peering of PSTN and/or On-Premises Peering PBX (formally referred to as Bring Your Own PBX - BYOP). Zoom Phone PSTN peering allows organizations to leverage their current carrier's PSTN environment for Zoom Phone connectivity. With this functionality, organizations can connect Zoom Phone with virtually any phone carrier.

About Ingate's SIParator® SBC product family.

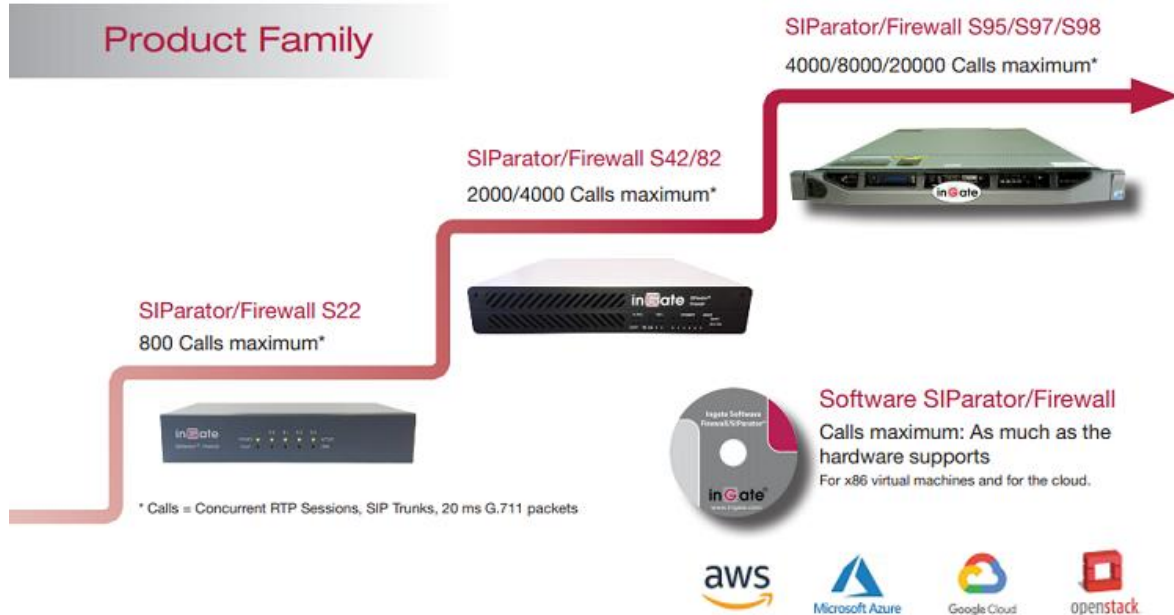
A session border controller is a device that connects to an existing network firewall to seamlessly enable SIP (Session Initiation Protocol) communications. While traditional firewalls block SIP traffic, including mission-critical applications such as Voice over IP (VoIP), Ingate's SIParator® SBC solves this problem, working in tandem with your current security solutions.

Ingate's SIParator® 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.

ZoomPhone Local Peering (BYOC and BYOP)

Ingate's firewall®, which is always included in the product, makes Ingate SIParator an all-in-one appliance for data security as well as session edge control.

Ingate SIParators/Firewalls® are available in a wide range of models®:



The SIParator simplifies SIP trunking and makes it easy to connect remote UC endpoints, aggregate SIP trunks, and distribute sessions between sites and service delivery points. It is used for real-time communications security, SIP interoperability, and extensive connectivity. The SIParator® is compatible with all existing networks and comes with a standard SIP proxy and SIP logger. It has support for NAT and PAT, as well as TLS and SRTP to encrypt both SIP signaling and media, eliminating the security issue most associated with using enterprise VoIP.

The flexible add-on licensing system allows any company to upgrade the SIParator®/Firewall® solution to meet their needs at any time.

With more than 10,000 installations worldwide, Ingate's SIParator® comes in a wide range of capacities and has been used by retail businesses, financial institutions, industrial companies, government agencies, call centers, and small and large businesses.

Deployment scenarios

Proof-of-concept topology

The interoperability between SIParator® SBC and Trunking with the Zoom phone system has been tested in the following configuration.

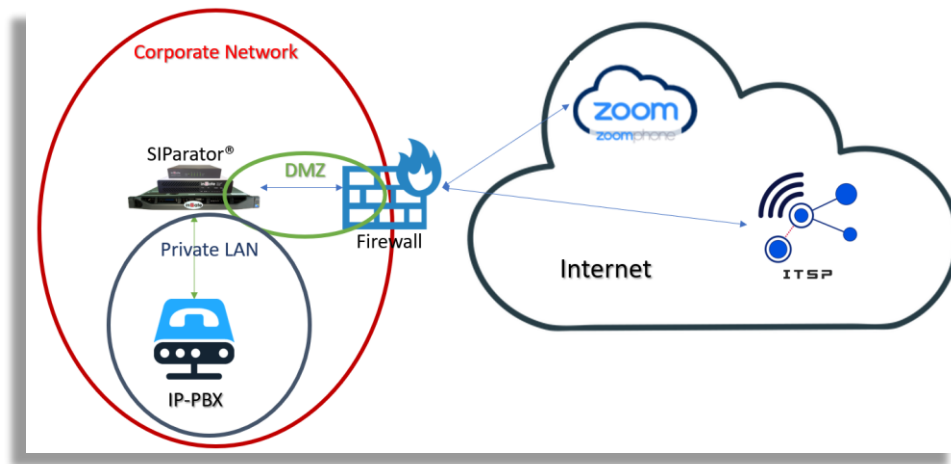


Figure 1: Implementation Design

The SIParator® configuration in this document will show how to route PSTN traffic to or from the existing customer's Zoom Phone system or PBX. It will also show how to route calls between Zoom users and PBX users (extensions)

We assume that SIParator will be located behind an existing firewall in a DMZ.

Our SIParator will be configured with 2 network interfaces enabled (it is strongly recommended not to use a single interface), one will be on the DMZ while the other will be on the internal private LAN where the IP PBX can be accessed.

Both the Zoom phone system and the SIP trunk provider are located on the WAN or an external network (Internet).

The IP-PBX is located on the Private Network

The Zoom phone system uses TLS signaling, while ITSP and IP-PBX use SIP over UDP

The Zoom phone system works with encrypted media (SRTP), while ITSP and IP-PBX use simple RTP for media.

Zoom Phone System Settings

For detailed instructions on how to set up your Zoom phone system, you can refer to the Zoom Help Center at

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

NOTE: Before you begin setup: ■ Contact your Zoom representative to enable SIP groups and configure SIP trunks that target your SBC for your Zoom Phone account. ■ Make sure you have Zoom Portal admin credentials. Please note that each customer must have a Zoom Phone administrator account and that all configuration related to Zoom Phone is done by the customer and not by the carrier.

Replace with application process to support BYOC and BYOP enablement

For more details see: [BYOC-P or BYOP-P deployment and connectivity options](#)

SIParator[®] SBC Configuration

Prerequisites

For this use case, validation has been performed with SIParator[®] version 6.4.1 and the minimum license required must include:

- Number of concurrent sessions of sip trunks. It is also known as CCS and must be at least the maximum number of concurrent SIP sessions that we want the solution mapped to 2 trunk groups to support.
- One trunk group will support simultaneous calls between PBX and PSTN and the second trunk will be associated with calls between Zoom and PSTN
- We also need to take into account the maximum number of simultaneous calls between Zoom and PBX, but they won't use any trunk groups.
- This can be achieved with shared CCS between the 3 streams (Zoom-PSTN, PBX-PSTN, Zoom-PBX). In this case you will need:

Total CCS needed = Zoom-PSTN + PBX-PSTN + Zoom-PBX

An additional trunk group that shares all CCS (license known as TGS)

If you have any doubts or questions about the best options for licensing, please feel free to send your questions to support@educronix.com

No other licenses are required for this specific use case. When transcoding is needed, no license is needed, as the transcoding feature is a purely software-based built-in functionality.

ZoomPhone Local Peering (BYOC and BYOP)

Make sure you are using one of the SIParator® appliances according to the expected workload, or an appropriately sized virtual machine if you are using software SIParator®

Before you start the deployment, make sure you have:

- A public IP address that will be used exclusively for your SBC. It can be mapped in your firewall and routed correctly to the IP address of SIParator® DMZ.
- Public certificates issued by one of the Zoom-supported CAs.

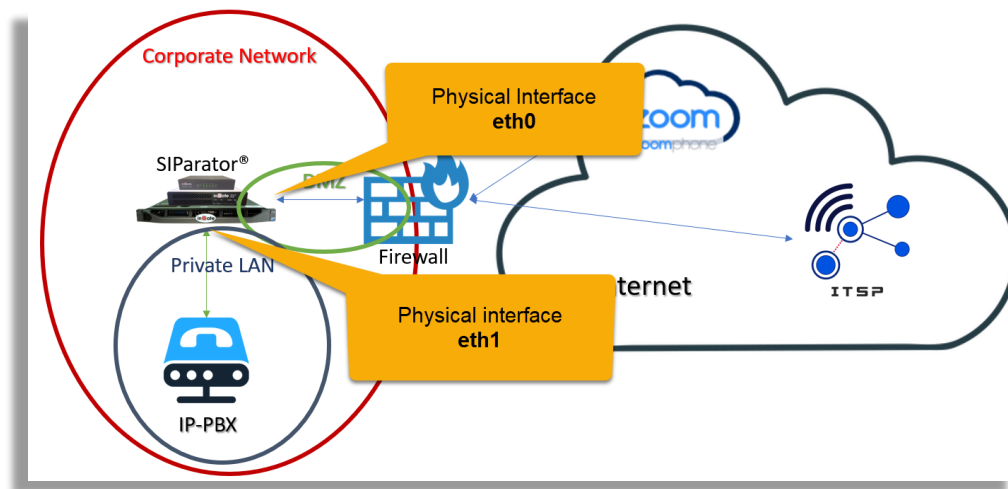
Configuring IP Network Interfaces

SBC interfaces will be assigned IP addresses to

- External interface. Which is located in the DMZ and is associated with the public IP address.
- Internal interface. Which will be used for management access to SIParator® and also to reach internal SIP resources (e.g. IP-PBX).

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

In our case, all interfaces are dedicated ethernet ports.



Configuring internal and external interfaces

You can use the tables provided by Zoom for signaling media and IPs. We will use the tables available at the time this document was created for Zoom documentation.

For signaling and Media, you can get the details of the IPs at this link: [BYOC-P or BYOP-P migration to the Common Platform](#)

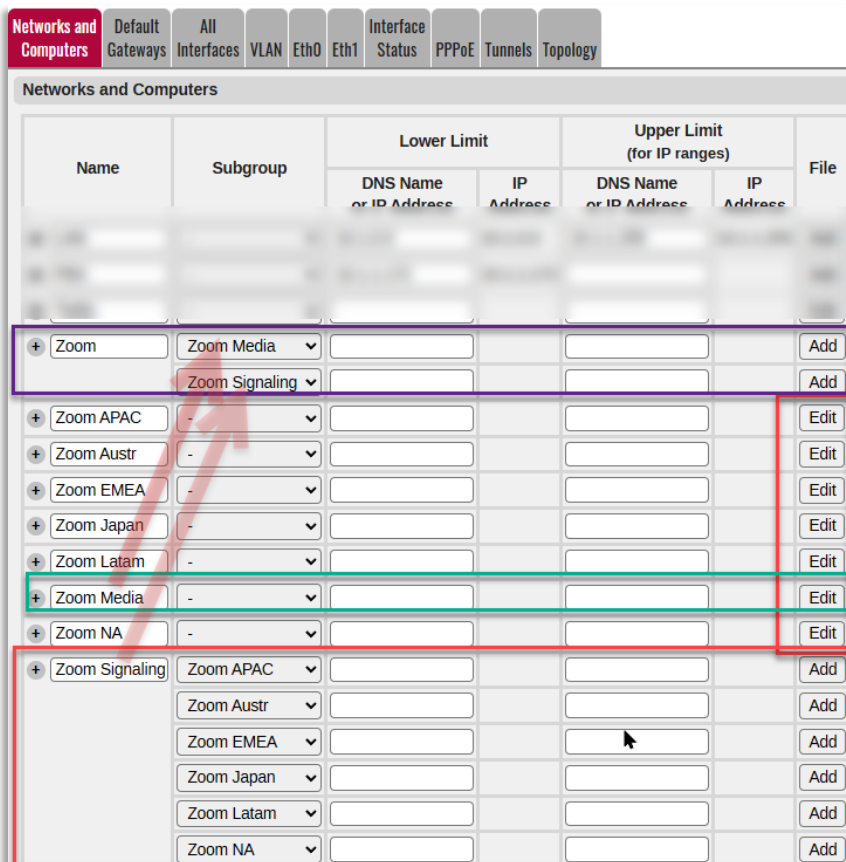
ZoomPhone Local Peering (BYOC and BYOP)

For the purposes of this document, we will select only the South America 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 in or deploying in.

Current Zoom Data Centers	Proposed new Zoom Data Centers
US01 - South America (SP/QR) <i>Mexico and Central America (Querétaro, MX)</i> Signaling IP: 149.137.69.247 Port: TCP/5061 Media Subnet: 149.137.69.0/24 Port: UDP/20000-64000 South America (São Paulo) Signaling IP: 64.211.144.247 Port: TCP/5061 Media Subnet: 64.211.144.0/24 Port: UDP/20000-64000	Zoom Common Platform - Central and South America Querétaro, MX Signaling IP: 159.124.128.84 Port: 5061 Media Subnet: 159.124.128.80/28 Port: 10000-65000 Dulles, VA, US Signaling IP: 206.247.121.212 Port: 5061 Media Subnet: 206.247.121.208/28 Port: 10000-65000

Since at the time of preparing this document the datacenters are in transition from the current location to the new one, we will use both groups of IPs for our configuration and thus have no dependence on when the migration is carried out.

To make this document more generic and make it easier for the reader to implement in any region, taking advantage of new Ingate functionalities that allow you to load IP tables as plain text, we will structure the network names as follows:



You can see that there is a line for each region, and each of them has an "edit" button enabled. This button is enabled when for any network name we choose the "add" button and add a table with a format explained in the ingate configuration manual here: [Ingate Reference Guide](#)

Here is the list of all text files containing such IP address configurations:

- APAC:
#APAC Old
149.137.41.246
207.226.132.198
#APAC New
170.114.156.212
170.114.185.212
- Australia:
#Australia Old
103.122.166.248
103.122.167.248
#Australia New
159.124.96.84
159.124.64.84
- EMEA:
#EMEA Old
213.19.144.198
213.244.140.198
#EMEA New
159.124.0.84
159.124.32.84
- Japan:
#Japan Old
209.9.211.198 #HK
101.36.167.237 #HK2
149.137.25.246
207.226.132.198
#Japan New
170.114.156.212
170.114.185.212
147.124.96.84
- Latam
#Latam Old
64.211.144.247
149.137.69.247
#Latam New
159.124.128.84
206.247.121.212
- North America NA
#North America Old
162.12.233.59
162.12.232.59

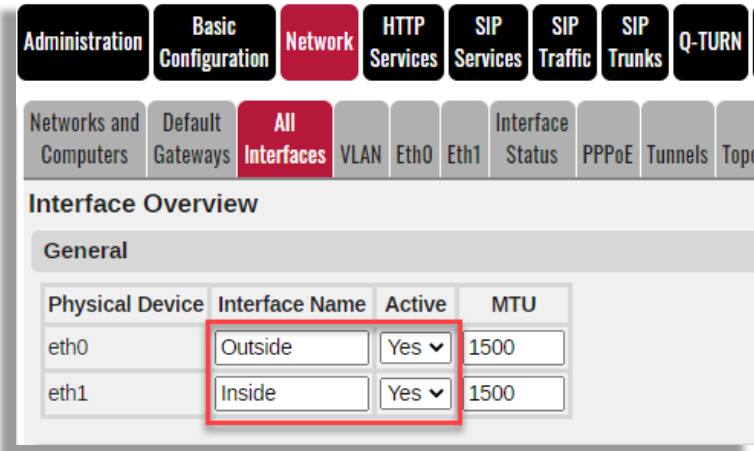
162.12.235.85
#North America New
144.195.121.212
206.247.121.212

For simplicity for Media we have consolidated all Media IPs into one name (Highlighted in green in the image above):

- Stocking
 - #North America
 - 162.12.232.0/24
 - 162.12.233.0/24
 - 162.12.235.0/24
 - #LATAM
 - 64.211.144.0/24
 - 149.137.69.0/24
 - #EMEA
 - 213.19.144.128/25
 - 213.244.140.0/24
 - #Australia
 - 103.122.166.0/24
 - 103.122.167.0/24
 - #APAC
 - 149.137.41.0/24
 - 207.226.132.0/24
 - #HK
 - 209.9.211.192/26
 - 101.36.167.0/24
 - #Japan
 - 207.226.132.0/24
 - 149.137.25.0/24
 - #New Media IP
 - 159.124.128.80/28
 - 101.36.167.0/24
 - 206.247.121.208/28
 - 144.195.121.208/28
 - 170.114.156.208/28
 - 170.114.185.208/28
 - 147.124.96.80/28
 - 159.124.96.80/28
 - 159.124.64.80/28
 - 159.124.0.80/28
 - 159.124.32.80/28

ZoomPhone Local Peering (BYOC and BYOP)

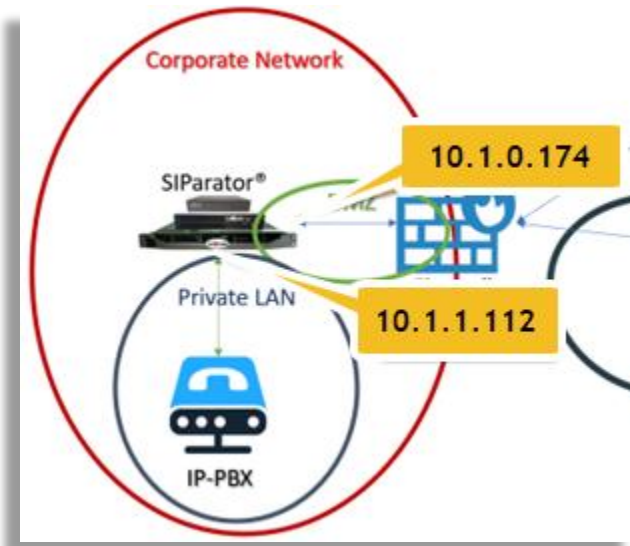
Make sure that 2 interfaces are enabled (active). In our case we are also assigning a name to each one (inside for eth1 and Outside for eth0)



The screenshot shows the configuration interface for SIPParator. The navigation menu includes Administration, Basic Configuration, Network (selected), HTTP Services, SIP Services, SIP Traffic, SIP Trunks, and Q-TURN. Under the Network section, the 'All' sub-menu is selected, leading to the 'Interfaces' page. The 'Interface Overview' table is as follows:

Physical Device	Interface Name	Active	MTU
eth0	Outside	Yes ▼	1500
eth1	Inside	Yes ▼	1500

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

ZoomPhone Local Peering (BYOC and BYOP)

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
eth0	Static	10.1.0.174	10.1.0.174	24	10.1.0.0	10.1.0.255	Outside (eth0)		-
eth1	Static	10.1.1.112	10.1.1.112	24	10.1.1.0	10.1.1.255	Inside (eth1)		-

Static route for the default gateway:

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		-	10.1.0.1	10.1.0.1	Outside (eth0)	<input type="checkbox"/>

Other network-related settings

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

inGate Zoom BYOC test

Administration | **Basic Configuration** | Network | HTTP Services | SIP Services | SIP Traffic | SIP Trunks | Q-TURN | Virtual Netw

Basic Configuration | Access Control | RADIUS | SNMP | Dynamic DNS Update | Certificates | ACME | TLS | Advanced Settings | SIP T

General

Name of this SIParator: Zoom BYOC te

Default domain: .

Version of Software SIParator/Firewall

Check for new versions of Software SIParator/Firewall: Yes No

Date of last successful version check: Not available

Software version in use: 6.4.1

Policy For Ping To the SIParator

Never reply to ping

Only reply to ping to the same interface

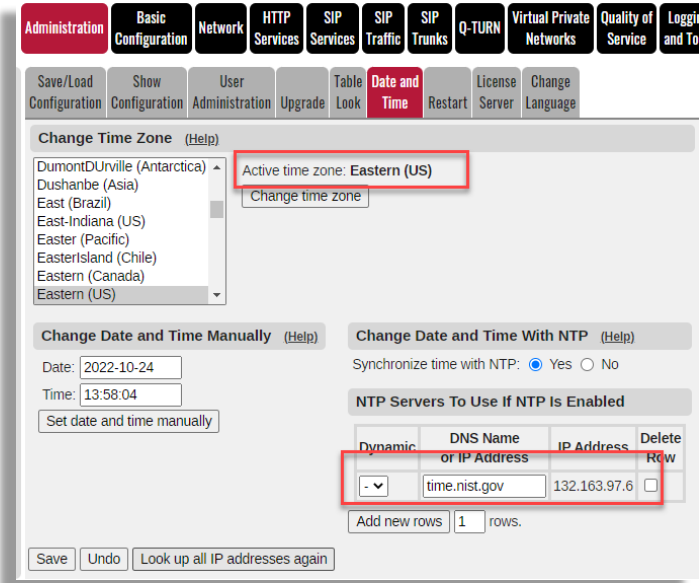
Reply to ping to all IP addresses

DNS Servers (Help)

No.	Dynamic	DNS Name or IP Address	IP Address	Delete Row
1	-	8.8.8.8	8.8.8.8	<input type="checkbox"/>

You can also name this SIParator. The name will be displayed in your browser tags.

Let's also assign an NTP server and a configuration time for the SIParator®. We assume that you are in the EST time zone.



Configuring TLS for Zoom

In this section, we'll enable TLS to set up connectivity to the Zoom phone system.

To enable TLS, we'll need the appropriate public certificates. With SIParator there are two ways to acquire, install, and maintain TLS certificates.

- **I use CSRs.** Generating the Signature Request from the SIParator, send it to the Certificate Authority to obtain the signed certificate and intermediate certificates (if necessary) and install them on the SIParator®.
- **Use of ACME.** Use SIParator built into the ACME client and use the appropriate ACME-enabled authority in accordance with Zoom-accepted CAs.

Use of CSR

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

Under Basic Configuration Certificates → Private → Certificates, add a new row:

ZoomPhone Local Peering (BYOC and BYOP)

Administration Basic Configuration Network HTTP Services 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.

- This page contains an error.

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

Private Certificates (Help)

Name	Certificate	Information	ACME Domain	Delete Row
No certificate exists.				
No value given.				
	Create New Import View/Download	No current certificate	-	<input type="checkbox"/>

Give it a name and click "Create New"

Fill in the requested information and ensure that the DNS of the Common Name extension and SubjectAltName points to the SIParator FQDN that resolves to the public IP address associated with the external interface:

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 can be imported into the system.

Expire in (days): * 365 Country code (C): US Organization (O): Educronix
Common Name (CN): zoom.educronix.com State/province (ST): FL Organizational Unit (OU): Engineering
Email address: ernesto@educr 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: zoom.educronix.com IP:

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

All remaining fields can be left at the default values.

Click "Create an X.509 Certificate Request"

ZoomPhone Local Peering (BYOC and BYOP)

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:

ACME

Use the ACME protocol for this X.509 certificate request: Yes No

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

*

Fields marked with "*" are mandatory.

The certificate request will be displayed as follows:

Apply changes

Administration **Basic Configuration** **Network** **HTTP Services** **SIP Services**

Changes have been made to the p

Save/Load Configuration (Help) On e On t New

seconds

Go back to the certificate and click "View/Download"

ZoomPhone Local Peering (BYOC and BYOP)

The screenshot shows the SIPParator web interface. At the top, there is a navigation menu with buttons for Administration, Basic Configuration, Network, HTTP Services, SIP Services, SIP Traffic, SIP Trunks, Q-TURN, Virtual Private Networks, Quality of Service, Logging and Tools, About, and Log out. Below this is a secondary menu with buttons for Basic Configuration, Access Control, RADIUS, SNMP, Dynamic DNS Update, Certificates, ACME, TLS, Advanced Settings, and SIPParator Type. The main content area is titled 'Private Certificates (Help)'. It contains a table with columns for Name, Certificate, and Information. The first row has 'byoc-cert' in the Name column, 'Create New' and 'Import' buttons in the Certificate column, and a 'View/Download' button in the Information column. The 'View/Download' button is highlighted with a red box. To the right of the table, the certificate details are visible: Subject: /C=US/ST=FL/L=Weston/O=Educronix/OU=Engineering/CN=byoc.edx-labs.com/emailAddress=ernesto@educronix.com and SubjectAltName: DNS:byoc.edx-labs.com.

Download the certificate in PEM or DER format. It will depend on the CA you are going to use to sign it and which one suits you best. We'll use PEM for our example.

The screenshot shows the 'Current Private Certificate for "byoc-cert"' page. It displays the current certificate request details: Subject: /C=US/ST=FL/L=Weston/O=Educronix/OU=Engineering/CN=byoc.edx-labs.com/emailAddress=ernesto@educronix.com and SubjectAltName: DNS:byoc.edx-labs.com. Below the details are three buttons: 'Download certificate/certificate request (DER format)', 'Download certificate/certificate request (PEM format)', and 'Return to certificate page'. The 'Download certificate/certificate request (PEM format)' button is highlighted with a red box.

The downloaded file should look like this:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDDDCCAFQCAQAwgZcxZAJBgNVBAYTA1VTMQswCQYDVQQIEwJGTDEPMA0GA1UE
-----
kAI2B3mQyjs2J4Ac65G548HEhmIkGx94oIhjq60Kgx47aDYQVQV263OYq6+8NV35
s7b+UOfjqGsz7+m/g/PZiw6Rvh2fVM2V+Uuj5d9j3TTweRjhb7V325NEmdw/SXCr
SO6K0CZWyl5sr5mv6FQUNw==
-----END CERTIFICATE REQUEST-----
```



Use it to request the signed certificate from the certificate authority you selected.

Once signed you will be provided with a set of files, usually 2:

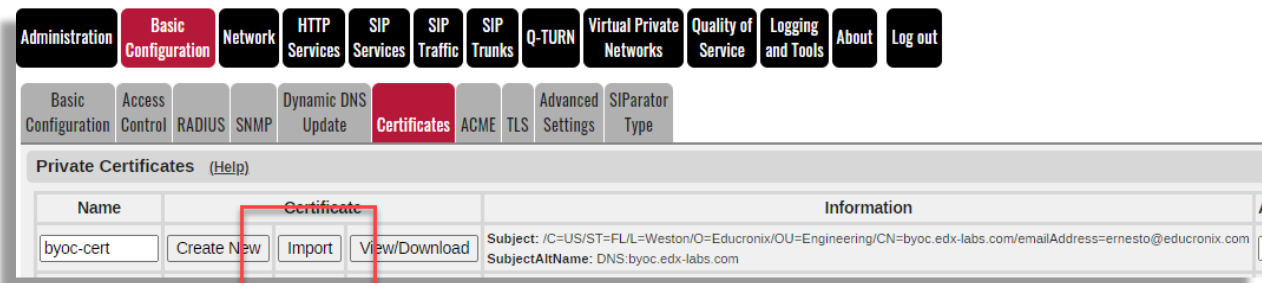
ZoomPhone Local Peering (BYOC and BYOP)

- Signed certificate
- Broker package certificates.

Similar to this:

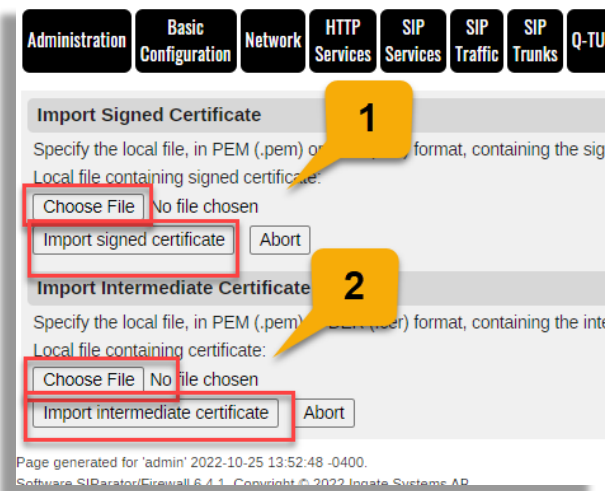
<input checked="" type="checkbox"/>		byoc_edx-labs_com.ca-bundle	10/21/2022 1:47 PM	CA-BUNDLE File	5 KB
<input checked="" type="checkbox"/>		byoc_edx-labs_com.crt	10/21/2022 1:47 PM	Security Certificate	3 KB

You will need to upload the signed certificate as well as the CA package as intermediate certificates. Use the "Import" button to do so:



The screenshot shows the SIPParator web interface. The navigation menu includes Administration, Basic Configuration, Network, HTTP Services, SIP Services, SIP Traffic, SIP Trunks, Q-TURN, Virtual Private Networks, Quality of Service, Logging and Tools, About, and Log out. The 'Basic Configuration' menu is expanded to show sub-menus: Basic Configuration, Access Control, RADIUS, SNMP, Dynamic DNS Update, Certificates, ACME, TLS, Advanced Settings, and SIPParator Type. The 'Certificates' sub-menu is selected, displaying the 'Private Certificates' page. A table lists certificates, with one entry named 'byoc-cert'. The 'Import' button in the table is highlighted with a red box.

First import the certificate, save and apply it, and then upload the package.

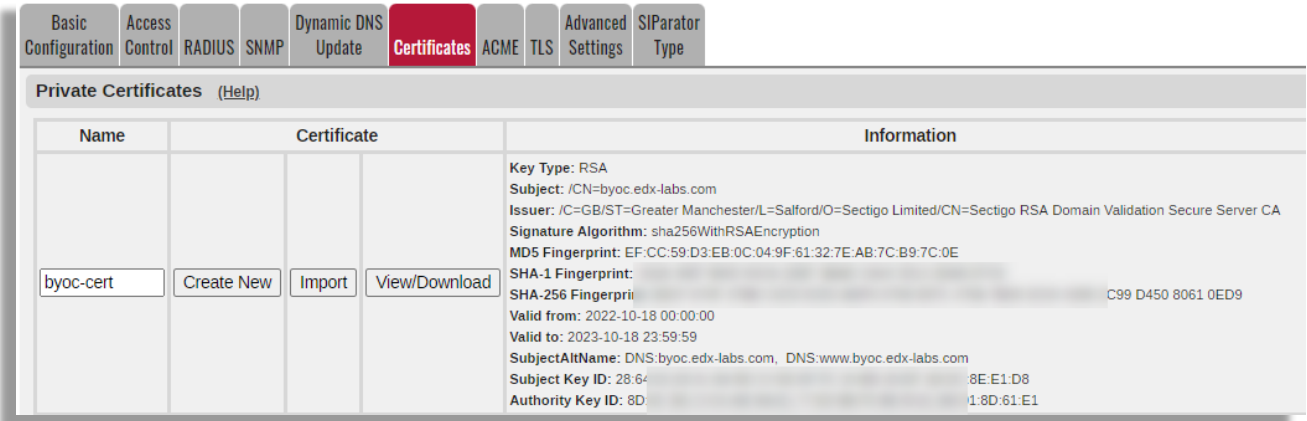


The screenshot shows the 'Import Signed Certificate' dialog box. The 'Choose File' button is highlighted with a red box and a yellow callout '1'. The 'Import signed certificate' button is highlighted with a red box and a yellow callout '2'. The dialog box contains the following text: 'Specify the local file, in PEM (.pem) or PKCS#12 (.p12) format, containing the signed certificate. Local file containing signed certificate: Choose File No file chosen Import signed certificate Abort'. Below this, there is another section for 'Import Intermediate Certificate' with similar text and buttons.

Save and reapply your changes.

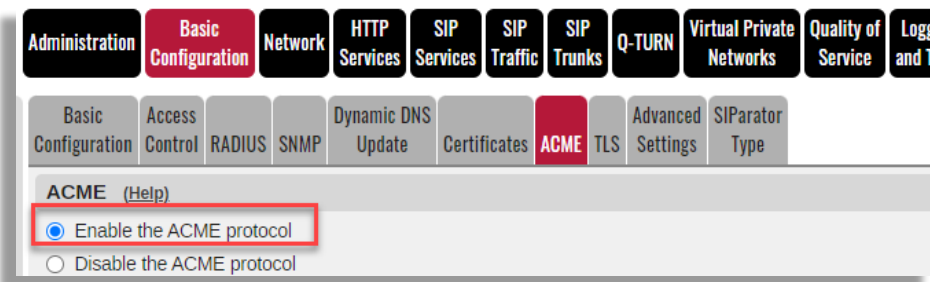
You should be able to see the new certificate signed similar to this:

ZoomPhone Local Peering (BYOC and BYOP)



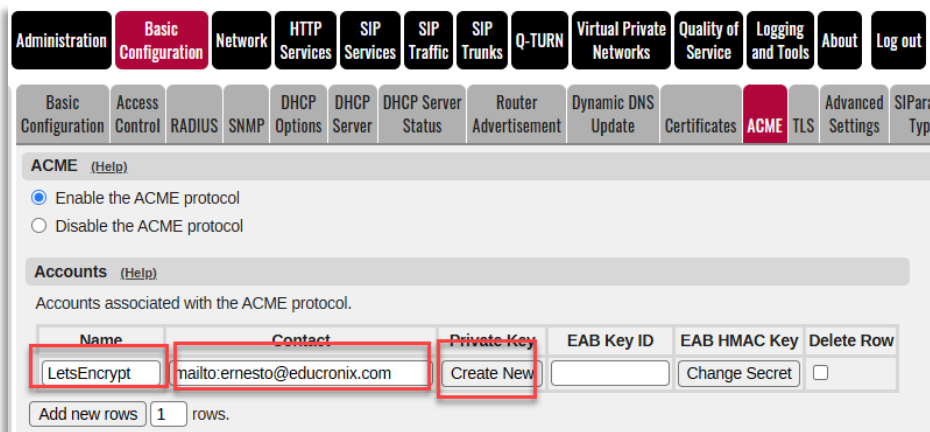
Using ACME

Before creating the certificate, we will need to have the SIPParator® ACME feature enabled and configured correctly.



For the purposes of this document, we have selected a Certificate Authority that supports the ACME protocol and meets Zoom's requirements.

In our case we will use Let's Encrypt which we have confirmed works correctly with Zoom.



- Name

ZoomPhone Local Peering (BYOC and BYOP)

- Add contact information in the format <mailto:xxxxx@yyyy.zzz> to provide who will receive updates and notifications from the CA.
- Generate a "Private Key" by pressing "Create New"

Add the service

Name	Domain or IP	Directory Path	Trusted CA	Delete Row
LetsEncrypt	acme-v02.api.letsencrypt.org	directory	-	<input type="checkbox"/>

Add new rows rows.

- Assign a name
- Enter the domain provided by the CA (for Let's Encrypt it's "acme-v02.api.letsencrypt.org")
- Enter the directory path as provided by the CA (for Let's Encrypt it's "directory")

Add a domain name to be used and referenced when creating new ACME-managed certificates.

Name	HTTP-01 Challenge Address	Service	Account	Renewal Interval (%)	Delete Row
EducronixAcme	eth0 (10.1.0.174)	LetsEncrypt	LetsEncrypt	67	<input type="checkbox"/>

- Assign a name
- Select the interface that will be facing outwards (Internet)
- Select the service and account (previously created).
- Keep the default value of 67% to set when the renewal request will be activated

Now we are ready to create the certificate using ACME.

As in "Using CSR" we will create a Certificate Signing Request, but in this case we will select the ACME tag.

Add a new row under Private Certificates and give it a name, click "Create New":

Name	Certificate	Information	ACME Doma
byoc.edx-labs	Create New	No current certificate	-

Key Type: RSA

Complete the information here:

Create Certificate or Certificate Request

Fill in the certificate data for "byoc.edx-labs" below, then create either a certificate or a certificate request. After generating a certificate request, and having it signed by a signing authority, you can create a certificate.

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 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:

Notice:

- Expiration and Common Name are required fields, however, the certificate authority will define Expiration regardless of the value you enter.
- The common name and DNS must match the FQDN associated with the SIParator®'s public IP address.

ACME

Use the ACME protocol for this X.509 certificate request: Yes No

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

* 2

Fields marked with "*" are mandatory.

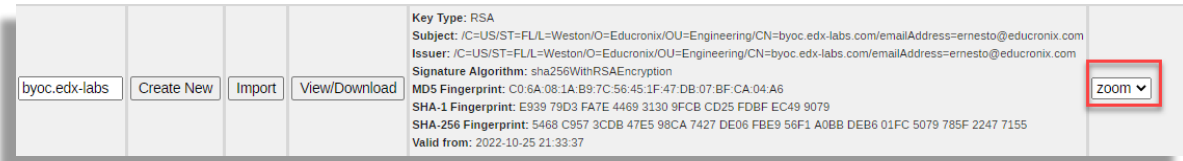
Page generated for 'admin' 2022-10-26 08:41:07 - 0400

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

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

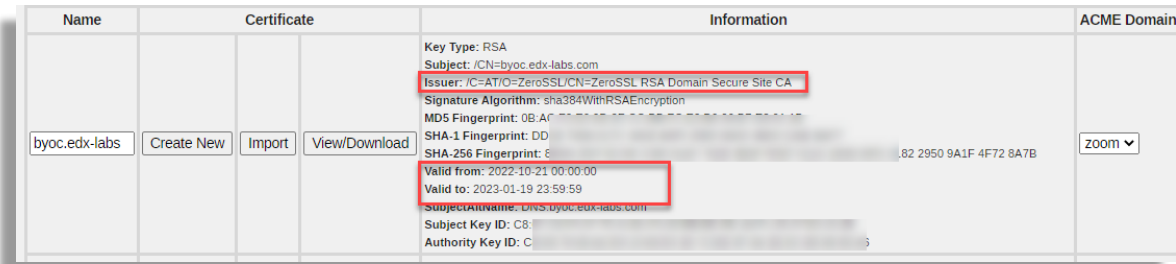
Be sure to associate the ACME domain with this new certificate.

ZoomPhone Local Peering (BYOC and BYOP)



Save and apply changes

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



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



Notice The USERTrust RSA Certificate Authority is included in the CAs accepted by Zoom.

If you have questions about other ACME options, please feel free to send your inquiries to support@educronix.com

Adding Zoom CA certificates to trust TLS connections

At the time this document is published, all Zoom certificates are signed by Digicert. You must add all Digicert root certificates in the CA section of the SIParator® basic configuration.

Here you just need to add a package that includes DigiCert root certificates. A good source for this pack can be found here: <https://curl.se/docs/caextract.html>

Or you can download all the necessary CA root certificates for DigiCert directly here:

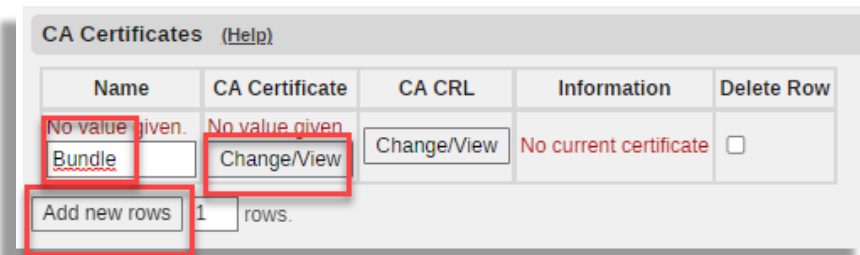
<https://cacerts.digicert.com/DigiCertGlobalRootCA.crt.pem>

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

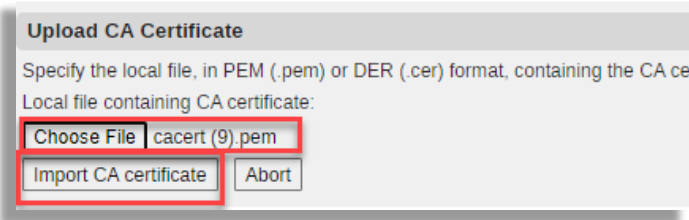
<https://cacerts.digicert.com/DigiCertGlobalRootG3.crt.pem>

In any case, to install any of the specific Bundles or Cas certificates mentioned above, you can do so here:

Under Basic Configuration Certificates → , in the CA Certificate section:

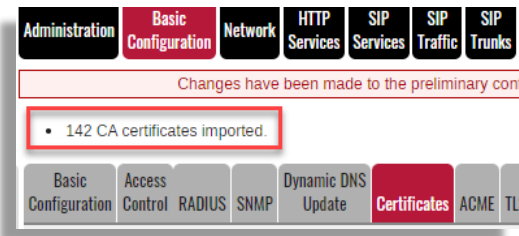


- Give it a name (Bundle in our case)
- Click CA Certificate "Change/View"



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

In the case of the package, you will see around 142 certificates uploaded with the same name.



Apply and save your changes.

Configure the NTP server

To have SIParator® well synced with your time zone, make the correct settings here:

The screenshot shows the SIParator configuration interface with the 'Date and Time' tab selected. The 'Change Time Zone' section has a dropdown menu set to 'Eastern (US)' and a 'Change time zone' button. The 'Change Date and Time With NTP' section has 'Synchronize time with NTP' set to 'Yes'. Below this, the 'NTP Servers To Use If NTP is Enabled' table is visible, containing one row with the following data:

Dynamic	DNS Name or IP Address	IP Address	Delete Row
<input type="checkbox"/>	time.nist.gov	132.163.97.6	<input type="checkbox"/>

At the bottom of the table, it says 'Add new rows 1 rows.'

Configuring TLS with Zoom Supported Versions

Zoom is known to only support TLS v1.2. In this section, we will create a TLS profile that includes only TLSv1.2 and will be used in the TLS for SIP configuration later in this document.

ZoomPhone Local Peering (BYOC and BYOP)

The screenshot shows the configuration interface for Zoom Phone. The top navigation bar includes tabs for Administration, Basic Configuration (selected), Network, HTTP Services, SIP Services, SIP Traffic, SIP Trunks, Q-TURN, Virtual Private Networks, Quality of Service, Logging and Tools, and About. Below this, there are sub-tabs for Basic Configuration, Access Control, RADIUS, SNMP, Dynamic DNS Update, Certificates, ACME, TLS (selected), Advanced Settings, and SIParator Type.

The main content area is divided into two sections:

- TLS Settings (Help)**: A table with columns: Name, Protocols, Ciphers, Diffie-Hellman Group, ECDH Curve, and Delete Row. The table contains several rows, with the row for "TLSv1.2" highlighted by a red box and a yellow callout labeled "2".
- Protocols (Help)**: A table with columns: Name, Protocol, and Delete Row. The table contains several rows, with the row for "TLSv1.2" highlighted by a red box and a yellow callout labeled "1".

At the bottom of each section, there are controls for adding new rows or groups.

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

SIP Configuration in SIParator®

Now we'll configure all signaling-related settings for SIP.

Configuring TLS Signaling

The screenshot displays the configuration interface for SIParator®. The 'Signaling Encryption' tab is selected. The 'Enable signaling encryption' option is checked. The 'TLS Connections On Different IP Addresses' section contains a table with the following data:

IP Address	Own Certificate	Use CN FQDN	Require Client Cert	TLS	Delete Row
eth0 (10.1.0.174)	byoc-cert	No	Yes	TLSv1.2	<input type="checkbox"/>

Below the table, the 'Default own certificate' is set to 'byoc-cert' and 'Use TLS' is set to 'TLSv1.2'. The 'TLS CA Certificates' section shows a row with 'CA' set to 'BundleCA' and 'Delete Row' as an unchecked checkbox.

- Add a new row in "TLS connections on different IP addresses"
- Associate your external interface (eth0) to receive and generate TLS traffic
- Select the certificate to be submitted by SIParator® (the one we created earlier).
- Disable "Use CN FQDN" and enable "Require Client Certificate" to meet Zoom MTLS support requirements.
- Select the newly 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 earlier.

It will also leave the following two settings at "No" as shown here:

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

SIP Port Configuration

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

Go to Basic SIP Services Settings →

Administration Basic Configuration Network HTTP Services **SIP Services** SIP Traffic SIP Trunks Q-TURN Virtual Private Networks Quality of Service

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

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

SIP Module [\(Help\)](#)

Enable SIP module

Disable SIP module

SIP Signaling Ports [\(Help\)](#)

Active	Port	Transport	Intercept	Allow From/To	Comment	Delete Row
Yes	5060	UDP and TCP	Yes	-		<input type="checkbox"/>
Yes	5061	TLS	Yes	Zoom Latam		<input type="checkbox"/>

Add new rows rows.

SIP Media Port Range [\(Help\)](#)

Ports: -

Public IP Address for NATed SIP Parator [\(Help\)](#)

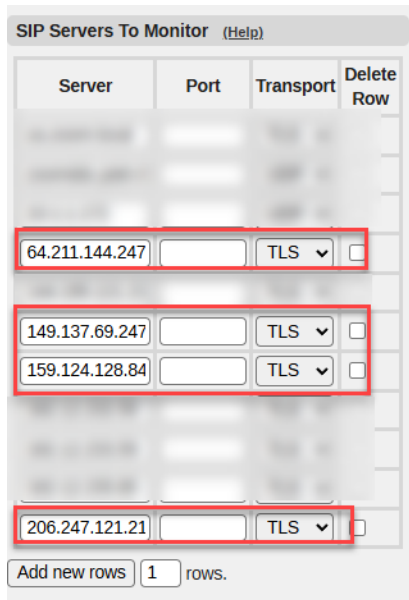
DNS Name	IP Address
<input type="text" value=""/>	<input type="text" value=""/>

- Make sure the 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. Later on, we can restrict this to only the sources we trust for UDP or TCP.

ZoomPhone Local Peering (BYOC and BYOP)

- Enable port 5061 for TLS, enable Intercept to restrict for traffic that only comes from the Zoom zone you defined earlier (in our case we create a network name "ZS LATAM" and we will restrict or allow only from those IPs).
- Since our SIParator® is located in a DMZ, the public IP is NATed and we need to note the public IP address as indicated.

At this point, we also want to monitor Zoom's SIP proxy IP addresses. In our case, we know that LATAM uses the following. SIParator® will monitor those IPs by periodically sending SIP OPTIONS.



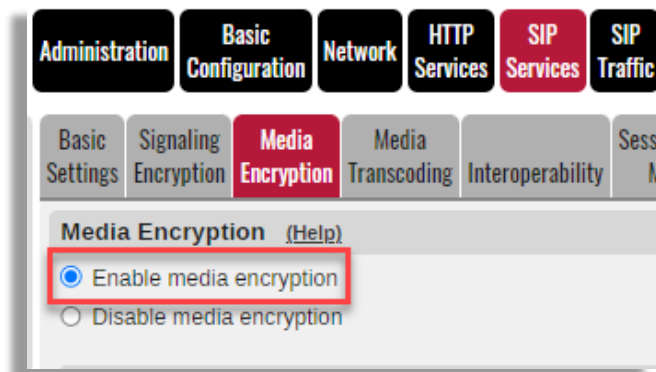
We are then monitoring the nodes corresponding to Latam as initially explained.

Because Zoom uses port 5061, you don't need to explicitly specify any ports to monitor (5061 is the default for TLS). We just need to select TLS.

Configure media encryption

Zoom requires, in addition to TLS as signaling encryption, the media that is also to be encrypted (SRTP)

To configure media encryption, make sure it is enabled:



Then we'll create a Crypto Suite group specifically for Zoom

ZoomPhone Local Peering (BYOC and BYOP)

Name	Suite	Delete Row
+ Any (transcode)	Cleartext (no encryption)	<input type="checkbox"/>
	SRTP sdesc. (AES-CM 128, SHA1 32)	<input type="checkbox"/>
	SRTP sdesc. (AES-CM 128, SHA1 80)	<input type="checkbox"/>
+ Cleartext	Cleartext (no encryption)	<input type="checkbox"/>
+ DTLS-SRTP	DTLS-SRTP	<input type="checkbox"/>
+ Encrypted (tran	SRTP sdesc. (AES-CM 128, SHA1 32)	<input type="checkbox"/>
	SRTP sdesc. (AES-CM 128, SHA1 80)	<input type="checkbox"/>
+ SRTP	SRTP sdesc. (AES-CM 128, SHA1 32)	<input type="checkbox"/>
	SRTP sdesc. (AES-CM 128, SHA1 80)	<input type="checkbox"/>
	SRTP sdesc. (AES-f8 128, SHA1 80)	<input type="checkbox"/>
+ SRTP Zoom	SRTP sdesc. (AES-CM 256, SHA1 80)	<input type="checkbox"/>
	SRTP sdesc. (AES-CM 128, SHA1 32)	<input type="checkbox"/>
	SRTP sdesc. (AES-CM 128, SHA1 80)	<input type="checkbox"/>

- Add a row with 3 sub-rows
- Select each sub-row associated with the suites shown in the image

Add a media encryption policy:

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

- Add a new row
- Select the added network called "zoom"
- Select TLS for the transport protocol
- Associate the newly created suite called "SRTP Zoom"
- Enable "Allow Transcoding"

Define a default encryption policy for everything else:

Suite requirements: Allow transcoding: Yes No

- Select "Clear Text" as the default policy (Clear Text means "No Encryption")
- Allow transcoding

Set the remaining parameters as shown:

The screenshot shows the following configuration options:

- Require TLS:** Require TLS for all cryptos but cleartext
- RTP Profile:** Prefer RTP/AVP (cleartext and legacy encryptions)
- Multi Profile:** Disable Multi Profile
- DTLS-SRTP:**
 - DTLS: DTLsv1.x
 - Add the client's IP to the cookie: Yes
 - Ignore invalid dates in the client's certificate: No
- Keep Established Crypto Within a Dialog:** No
- Add Cryptos in the B2BUA:** Yes
- Force Media Encryption:** No

Defining DNS Override to Handle Traffic Distributed to Zoom with Failover or Balancing

In this section we will take advantage of a functionality of the SBC that allows you to define a url and associate a distribution table very similar to an IP address table with SRV type records.

This allows us to target all the Zoom proxies we want to use as potential targets and allows us to set weights and priorities for traffic distribution.

Let's look at an example of the table in the SIP Traffic → Routing section

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

Methods Filtering Local Registrar Authentication Accounts STIR Call Control Dial Plan **Routing** Accounting Classes IDS/IPS Test Agent Status

DNS Override For SIP Requests (Help)

Domain	Relay To								Delete Row
	DNS Name or IP Address	IP Address	Port	Transport	Priority	Weight	Auth	Modify RURI	
+ us.zoom.local	64.211.144.247	64.211.144.247	5061	TLS	1	100	No	No	<input type="checkbox"/>
	149.137.69.247	149.137.69.247	5061	TLS	1	100	No	No	<input type="checkbox"/>
	159.124.128.84	159.124.128.84	5061	TLS	2	100	No	No	<input type="checkbox"/>
	206.247.121.212	206.247.121.212	5061	TLS	2	100	No	No	<input type="checkbox"/>

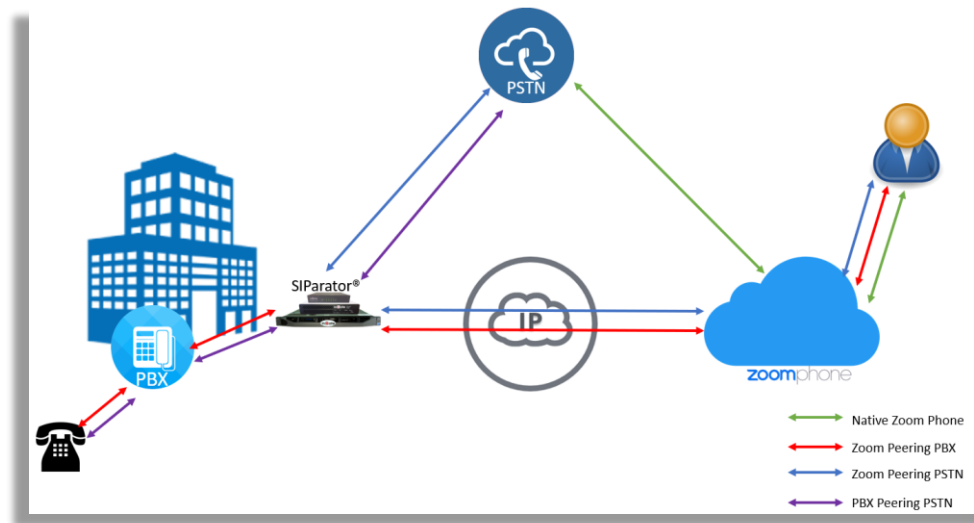
ZoomPhone Local Peering (BYOC and BYOP)

Here we have created a destination (url) called us.zoom.local which distributes with 2 different priorities (1 and 2) and proxy groups to which it is going to be distributed in round-robin using the indicated weights.

This should fit your particular Zoom traffic distribution strategy that best fits your strategy.

Configure SIP trunking

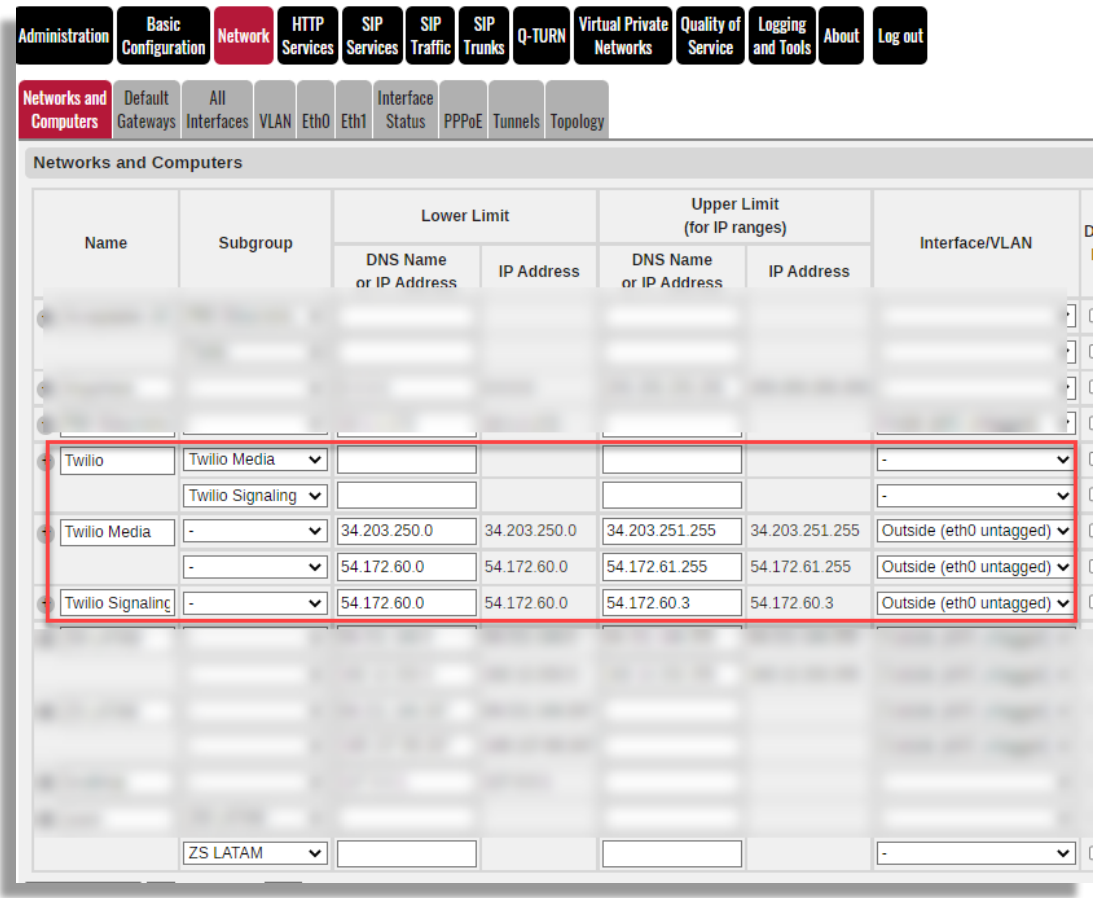
Let's understand what SIP flows look like in our case:



Configuring the Zoom-PSTN Trunk Group

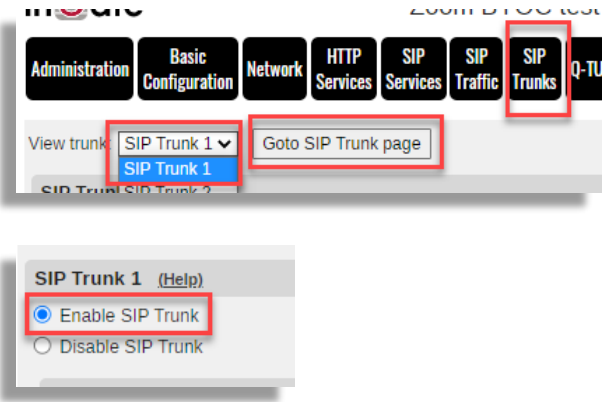
In our case, we are using Twilio's SIP trunking service for demonstration purposes.

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



Let's set up the trunk group

First, we'll enable a new trunk pool by enabling from the drop-down options:



ZoomPhone Local Peering (BYOC and BYOP)

Click "Go to SIP Trunks Page" and enable the Trunk Group

We are using Twilio's elastic SIP trunk service and have as an assigned FQDN:
zoompeering.pstn.twilio.com

To not define the trunk:

SIP Trunking Service [\(Help\)](#)

Use parameters from other SIP trunk
 Define SIP trunk parameters

Service name: (Unique descriptive name)

Service Provider Domain: (FQDN or IP address)

Restrict to calls from: (.' = No restriction)

Outbound Proxy: (FQDN or IP address)

Use alias IP address: (Forces this source address from our si

Outbound Gateway: (.' = Use Default Gateway)

Signaling Transport: (.' = Automatic)

Port number:

From header domain:

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

- Name the trunk group
- Use the provided proxy FQDN as the service provider's domain.
- Since our SIParator® is behind a firewall (DMZ), we'll need to enter the public IP in the hostname in Request-URI.

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

Relay media:

Service Provider domain is trusted:

Now we'll configure the matching rules to route the designated inbound DID's for Zoom or auto attendant users:

Main Trunk Line [\(Help\)](#)

No.	Reg	Display Name	User Name	Identity	User ID	Password	Incoming Trunk Match	Forward to
1	No		+19548668899	+19548668899		Change Password		

PBX Lines [\(Help\)](#)

No.	Reg	From PBX Number/User	Display Name	User Name	Identity	User ID	Password	Incoming Trunk Match	Forward to PBX Account	Delete Row
1	No					Change Password		(+19548668899)	\$1	<input type="checkbox"/>

Add new rows rows.

If you have more than one DID, you can continue to add rows to the PBX line table and match additional DID's. You can also use regular expressions for matching.

ZoomPhone Local Peering (BYOC and BYOP)

The DID configuration (E164 format) on the main trunk line (user and identity) will be used for caller identification purposes on outbound calls. In our case, we're using the DID assigned to the auto attendant in Zoom.

Assigned Unassigned Ported BYOC Cloud Peering

Main Company Number: Set

Add Import Export

Q Search Number Type (All) Assigned to (All) Status (All)

Assign SMS/MMS Disable SMS/MMS

<input type="checkbox"/>	Number	Area	Number Type	Capability	Assigned To	Number Status
<input type="checkbox"/>	(954) 852-8529	Fort Lauderdale, Florida, United States	Toll Number	Incoming & Outgoing	Main Auto Receptionist (Auto Receptionist) Ext. 801	Normal
<input type="checkbox"/>	(954) 852-8530	Fort Lauderdale, Florida, United States	Toll Number	Incoming & Outgoing	Ernesto Casas Ext. 800	Normal
<input type="checkbox"/>	(954) 866-8899	United States	Toll Number	Incoming & Outgoing	Main Auto Receptionist (Auto Receptionist) Ext. 801	Normal

We are now setting up the connection of this trunk group to Zoom.

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

Setup for the PBX (help)

Use PBX from other SIP trunk

Define PBX settings

PBX Name: Zoom peer (Unique descriptive name)

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

PBX Registration SIP Address	Authentication		PBX IP Address		PBX Domain Name
	User ID	Password	DNS Name or IP Address	IP Address	
		Change Password			us.zoom.local

(At least one of PBX Registration, IP address or Domain Name is required to locate the PBX)

PBX Network: Zoom Latam

Signaling transport: TLS (Automatic)

Port number:

Match From Number/User in field: From URI

Common User Name suffix:

To header field: Same as Request-URI

Forward incoming REFER: No

Send DTMF via SIP INFO: No

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

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

- Select "Define PBX Settings"
- Assign a name

- Under "PBX Domain Name" enter the url we created to define the traffic distribution strategy to Zoom (us.zoom.local)

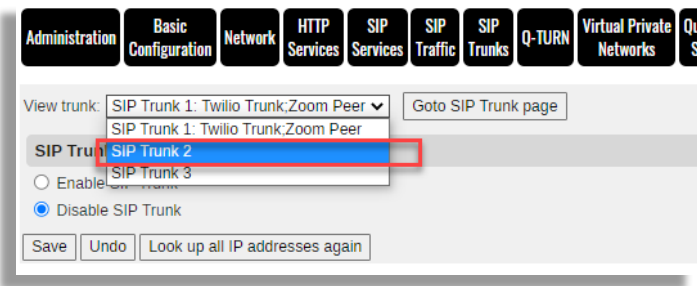
#Latam Old
64.211.144.247
149.137.69.247
#Latam New
159.124.128.84
206.247.121.212

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

PBX-PSTN Trunk Group Configuration

In this section we assume that the ITSP will also provide service for Trunking with DID's associated with the PBX; this way, you can use a single SIParator® 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 another SIP trunk". In this way we will use the same Trunk that we already configured in the previous section.

ZoomPhone Local Peering (BYOC and BYOP)

SIP Trunk 2 (Help)

Enable SIP Trunk
 Disable SIP Trunk

SIP Trunking Service (Help)

Use parameters from other SIP trunk
 Define SIP trunk parameters

SIP Trunk Parameters: Twilio Trunk

Main Trunk Line (Help)

No.	Reg	Outgoing Calls			Authentication		Incoming Calls	
		Display Name	User Name	Identity	User ID	Password	Incoming Trunk Match	Forward to
1	No		+19548667575	+19548667575		Change Password		

PBX Lines (Help)

No.	Reg	Outgoing Calls			Authentication		Incoming Calls	
		From PBX Number/User	Display Name	User Name	Identity	User ID	Password	Incoming Trunk Match
2	No					Change Password	+1(9548667575)	\$1

Add new rows: rows.

- Enable the trunk
- Use parameters from another SIP trunk and choose Twilio Trunk (configured in the previous section)
- We will use a different DID and add it to the outgoing username and identity for caller ID purposes.
- For the incoming call it will match the DID assigned to PBX Trunking. If you have a DID you can continue to add rows on the switchboard lines.

Now we will configure PBX connectivity

Setup for the PBX (Help)

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)

PBX Registration SIP Address	Authentication		PBX IP Address		PBX Domain Name
	User ID	Password	DNS Name or IP Address	IP Address	
		Change Password		10.1.1.172	

(At least one of PBX Registration, IP address or Domain Name is required to locate the PBX)

PBX Network: PBX Educronix

Signaling transport: - (':' = Automatic)

Port number:

Match From Number/User in field: From URI

Common User Name suffix:

To header field: Same as Request-URI

Forward incoming REFER: No

Send DTMF via SIP INFO: No

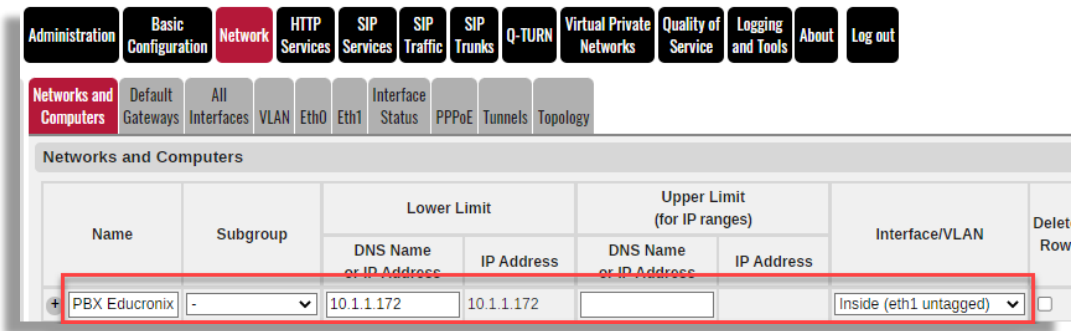
Remote Trunk Group Parameters usage: - (':' = Don't use TGP)

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

- Select "Define PBX Settings"
- Naming the PBX
- In PBX Domain enter the IP address of your PBX (In our case 10.1.1.172)

ZoomPhone Local Peering (BYOC and BYOP)

- Select the network name added earlier to → Network Networks and Computers. If you haven't already, see the following example:

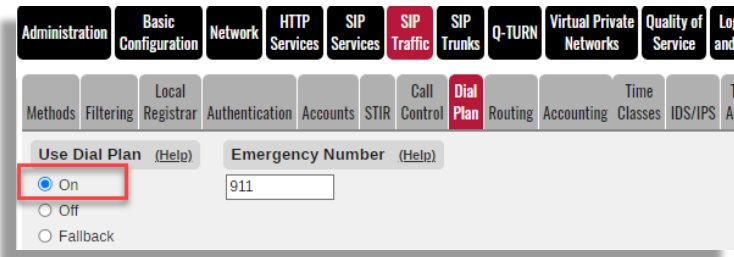


- Leave the remaining fields with the default values.

Configure the dial plan

With the dial plan, we will be able to route outbound traffic, traffic between Zoom and PBX and also enable SIParator® to respond to Zoom option requests.

First, you'll need to activate the dial plan.



Enabling SIP Options for Zoom Requests

We will need to detect OPTIONS requests landing on the external interface. SIP options send requests to the external public IP in a similar way to this:

```
recv from 149.137.69.247:30973 via 10.1.0.145:5061 TLS connection 7:
OPTIONS sip:3.217.32.189:5061 SIP/2.0
Via: SIP/2.0/TLS 149.137.69.247:5061;branch=z9hG4bK00Bf1f6d0bf4a6cc6c
From: <sip:149.137.69.247>;tag=gK0015c377
To: <sip:3.217.32.189>
Call-ID: 101654428_1298819240@149.137.69.247
CSeq: 343588 OPTIONS
Max-Forwards: 1
Allow: INVITE,ACK,CANCEL,BYE,REGISTER,REFER,INFO,SUBSCRIBE,NOTIFY,UPDATE,OPTIONS,MESSAGE,PUBLISH
Accept: application/sdp, application/isup, application/dtmf, application/dtmf-relay, multipart/mixed
Contact: <sip:149.137.69.247:5061>
Content-Length: 0
```

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

sip:@?34.195.141.39

In Dial Plan, match the request URI to the expression:

Name	Use This Or This	Delete Row
	Prefix	Head	Tail	Min. Tail	Domain	Req Expr	
Options			-			sip.@?34.198.141.39	<input type="checkbox"/>

- Name the rule
- Enter the regular expression.

Under Dial Plan → , add the rule to "Allow" Options.

No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment	Delete Row
					Forward	ENUM				
1	-	Options	Allow	-			-	-		<input type="checkbox"/>

Add new rows | 1 rows.

ZoomPhone Local Peering (BYOC and BYOP)

We will enter traffic identification rules coming from the PBX or Zoom using the From Header matching section.

Name	Use This Or This	Transport	Network	Delete Row
	Username	Domain	Reg Expr			
From LAN	*	*		UDP	LAN	<input type="checkbox"/>
Zoom Latam	*	*		TLS	Zoom Latam	<input type="checkbox"/>

The From LAN rule identifies all traffic coming from the Internal network and that includes the PBX and Zoom Latam identifies traffic coming from Zoom. In both cases, the source network is used to make the match.

Next, we'll use the Dial Plan for 3 main purposes:

- Route outbound traffic to PSTN from Zoom
- Routing Outbound Traffic to PSTN from PBX
- Route calls within the network between Zoom users and PBX users both ways

Zoom to PSTN Output Path

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

The screenshot shows the SIP configuration interface with the 'Dial Plan' tab selected. The 'Use Dial Plan' section is set to 'On' with an emergency number of '911'. Below it, the 'Matching From Header' table is visible, with a new row for 'Zoom Latam' highlighted by red boxes. The 'Zoom Latam' row has wildcards for Username and Domain, and is configured for TLS transport and the Zoom Latam network.

Name	Use This Or This	Transport	Network	Delete Row
	Username	Domain	Reg Expr			
Zoom Latam	*	*		TLS	Zoom Latam	<input type="checkbox"/>

- Add a row in the Match from header
- Name the rule
- Use the wildcard "*" for the username and domain.
- Select the transport protocol to be discovered (TLS)
- Select the network that the traffic will come from (Zoom signaling sources)

Add a request URI rule to match the received traffic to advance later to PSTN. Here we must take into account that calls to the PSTN can come from both Zoom and the PBX, therefore we will use a regular expression that validates that the destination is in 10-digit E.164 format and that it arrives either through the internal interface or through the Public IP:

sip:(\+1.....)@(10.1.1.112|34.195.141.39)

Name	Use This Or This	Delete Row
	Prefix	Head	Tail	Min. Tail	Domain	Reg Expr	
PSTN			-			sip:(\+1.....)@(10.1.1.112 34.195.141.39)	<input type="checkbox"/>

- Add a new row in "Matching Request-URI"
- Name the new rule
- Match SIP requests to [***sip:\(\+1.....\)@\(10.1.1.112|34.195.141.39\)***](#)
- Now we will define the destination to the PSTN trunk (forward to) using the Zoom-PSTN trunk group

Name	No.	Use This Or This		... Or This		Use Alias IP	Delete Row
		Account	Replacement Domain	Port	Transport	Reg Expr	Trunk		
PSTN Zoom		-			-		SIP Trunk 2: Twilio,Zoom peer	<input type="checkbox"/>	<input type="checkbox"/>

- Add a new row in the "Forward to" table
- Name the rule
- Select Trunk 2 as the target (the one we created with the ISTP for Zoom DIDs)

Next, let's define the actual dial plan rule for sending outbound traffic to PSTN from Zoom.

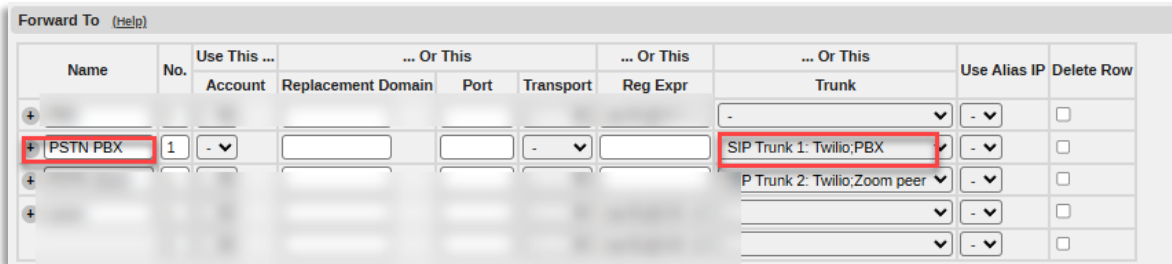
No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment	Delete Row
					Forward	ENUM				
5	Zoom Latam	PSTN	Forward	PSTN Zoom						<input type="checkbox"/>

- Create a rule where If **the From header** matches "Zoom Latam" and the **request URI** matches "PSTN", make a **Forward** to "PSTN Zoom"

PBX to PSTN Output Path

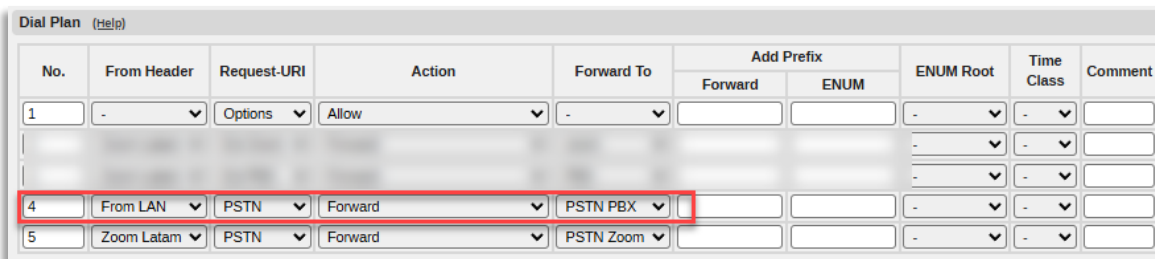
Now we're ready to add dial plan rules to route output to PSTN from PBX.

Add a "Forward to" rule that points to the trunk we created for PBX – PSTN connectivity.



- Add a new row in the "Forward to" table.
- Name the new rule
- Select Trunk 1 (the one we created earlier for PSTN connectivity for the PBX)

Add the actual dial plan routing rule:

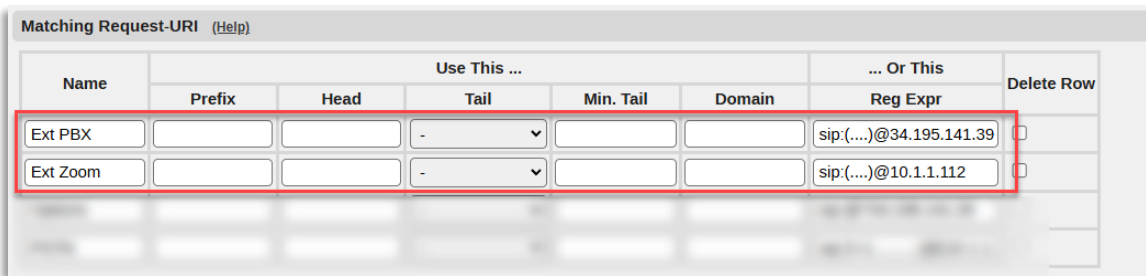


- Add a new row to "Dial Plan"
- Match **the From header** to the "From PBX" rule and **the request URI** to "To PSTN" and "Forward" to the previously created path named "To ITSP PBX"

The next step will be to add the routing rules needed to move traffic to the Zoom Users/Extensions
Users ↔ /PBX Extensions

Zoom PBX Path ↔

Here we will detect calls to Zoom extensions by matching a 4-digit number coming into SIParator® from the PBX, or matching it to a 4-digit number coming into SIParator® from Zoom.



ZoomPhone Local Peering (BYOC and BYOP)

- Add a new row to match dialing to a PBX extension. This call will arrive at the interface external to the SIParator®'s public IP address.
- Name the new row.
- Enter the matching string " sip:(...)@34.195.141.39"
- Add a new row to match the dialing to a Zoom extension. This call will arrive at the internal interface to the private IP address of the SIParator®.
- Name the new row.
- Enter the matching string " sip:(...)@10.1.1.112"

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

Forward To <small>(Help)</small>									
Name	No.	Use This Or This			... Or This	... Or This	Use Alias IP	Delete Row
		Account	Replacement Domain	Port	Transport	Reg Expr	Trunk		
+ PBX	1	-			-	sip:\$1@10.1.1.	-	-	<input type="checkbox"/>
+ PSTN PBX	1	-			-		SIP Trunk 1: Twilio;PBX	-	<input type="checkbox"/>
+ PSTN Zoom	1	-			-		SIP Trunk 2: Twilio;Zoom peer	-	<input type="checkbox"/>
+ zoom	1	-			-	sip:\$1@us.zoo	-	-	<input type="checkbox"/>

- Add a new row to define a route to the PBX
- Name the new row
- Use RegExp to define the destination: "sip:\$1@10.1.1.172; transport=udp; b2buawm"
- Assure that he added "; transport=udp; b2buawm" at the end of the expression.
- Add a new row where we'll use the url we created with DNS Override, to distribute traffic to Zoom extensions with the same strategy we defined for traffic from the PSTN. Let's use: "sip:\$1@us.zoom.local; b2buawm"

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

Dial Plan <small>(Help)</small>										
No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment	Delete Row
					Forward	ENUM				
1	-	Options	Allow	-			-	-		<input type="checkbox"/>
2	From LAN	Ext Zoom	Forward	zoom			-	-		<input type="checkbox"/>
3	Zoom Latam	Ext PBX	Forward	PBX			-	-		<input type="checkbox"/>
4	From LAN	PSTN	Forward	PSTN PBX			-	-		<input type="checkbox"/>
5	Zoom Latam	PSTN	Forward	PSTN Zoom			-	-		<input type="checkbox"/>

- Add 2 new rows, one for routing Zoom calls to PBX and the second for routing calls from PBX to Zoom.
- By matching **From Header** to "Zoom Latam" and **Request-URI** to "Ext PBX", forward the call to "PBX"
- When matching **From Header** to "From LAN" and **Request-URI** to "Ext Zoom", forward the call to "zoom"
- Ensure that the rules for extension have a value n in the numbering order lower than the corresponding rule for PSTN (as shown in the image above)

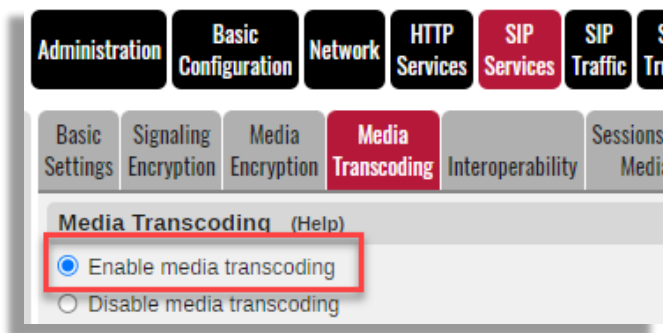
Transcoding settings

Local peering connections, both over the Internet and private circuit options, will prefer the following codecs in the order of preference listed below:

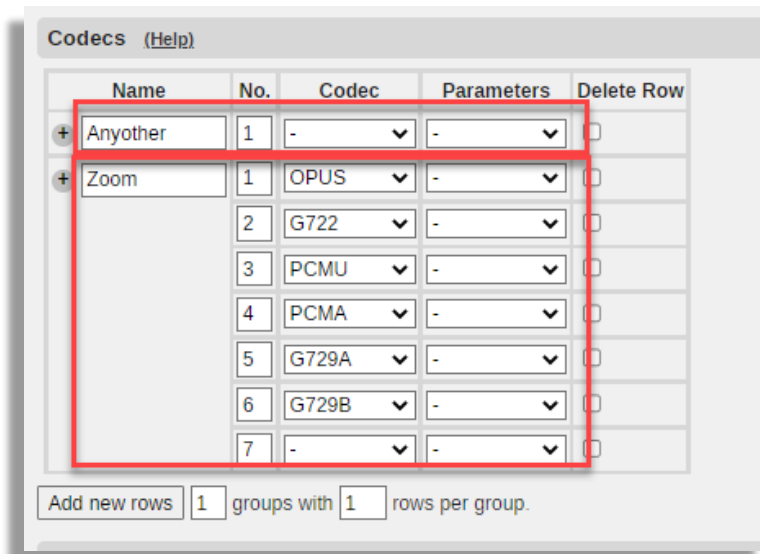
- OPUS
- G.722
- G.711A-law/ μ -law
- G.729

SIParator® has built-in software-based transcoding with no additional license required.

You'll need to enable transcoding:



First we'll create the necessary codec groups:

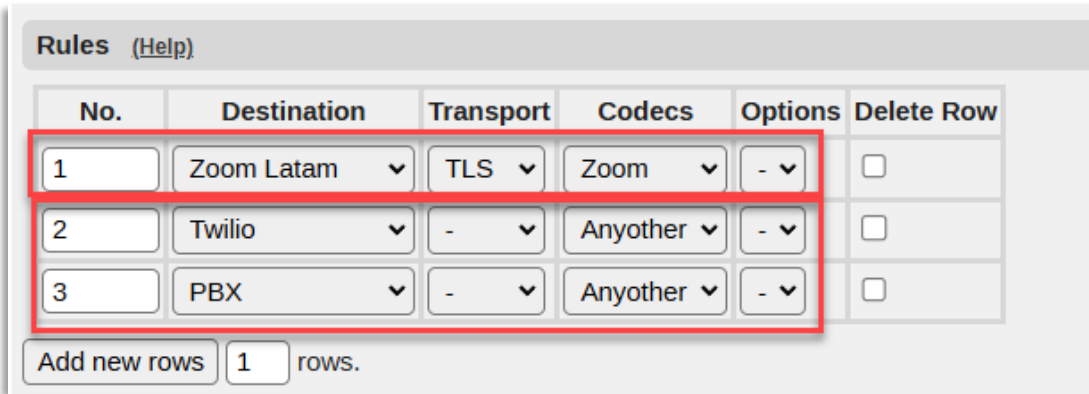


- Add 1 row and 1 additional row with 7 sub-rows.
- The first row, named Any Other in our example, will not have any selection in the Codec column. This means that any codec is compatible with the group.

ZoomPhone Local Peering (BYOC and BYOP)

- The second row, named Zoom, has a subrow for each Zoom-compatible codec, as mentioned above

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

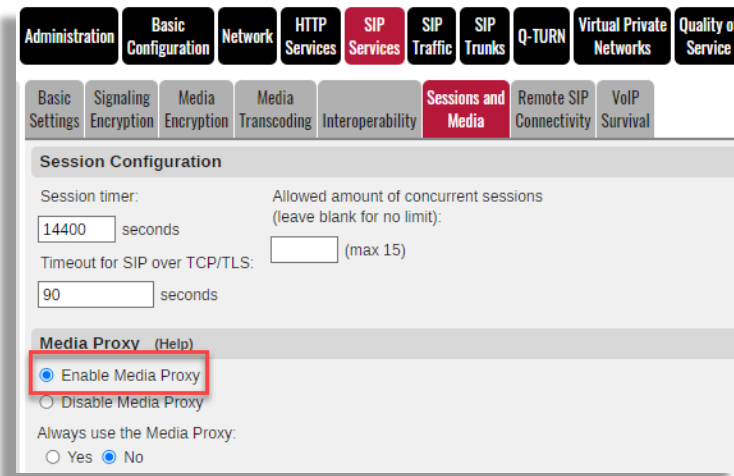


No.	Destination	Transport	Codecs	Options	Delete Row
1	Zoom Latam	TLS	Zoom	-	<input type="checkbox"/>
2	Twilio	-	Anyother	-	<input type="checkbox"/>
3	PBX	-	Anyother	-	<input type="checkbox"/>

Add new rows rows.

- For the Zoom signaling network, when using the TLS transport, attach the Zoom codec group.
- For Twilio (ISTP), for any transport, attach the codec group "Anyother".
- Same for "PBX Educronix".

Make sure the media proxy is enabled:



Administration Basic Configuration Network HTTP Services SIP Services SIP Traffic SIP Trunks Q-TURN Virtual Private Networks Quality of Service

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

Session Configuration

Session timer: 14400 seconds Allowed amount of concurrent sessions (leave blank for no limit): (max 15)

Timeout for SIP over TCP/TLS: 90 seconds

Media Proxy (Help)

Enable Media Proxy
 Disable Media Proxy

Always use the Media Proxy:
 Yes No

Final recommendations and other points of interest

Useful documentation

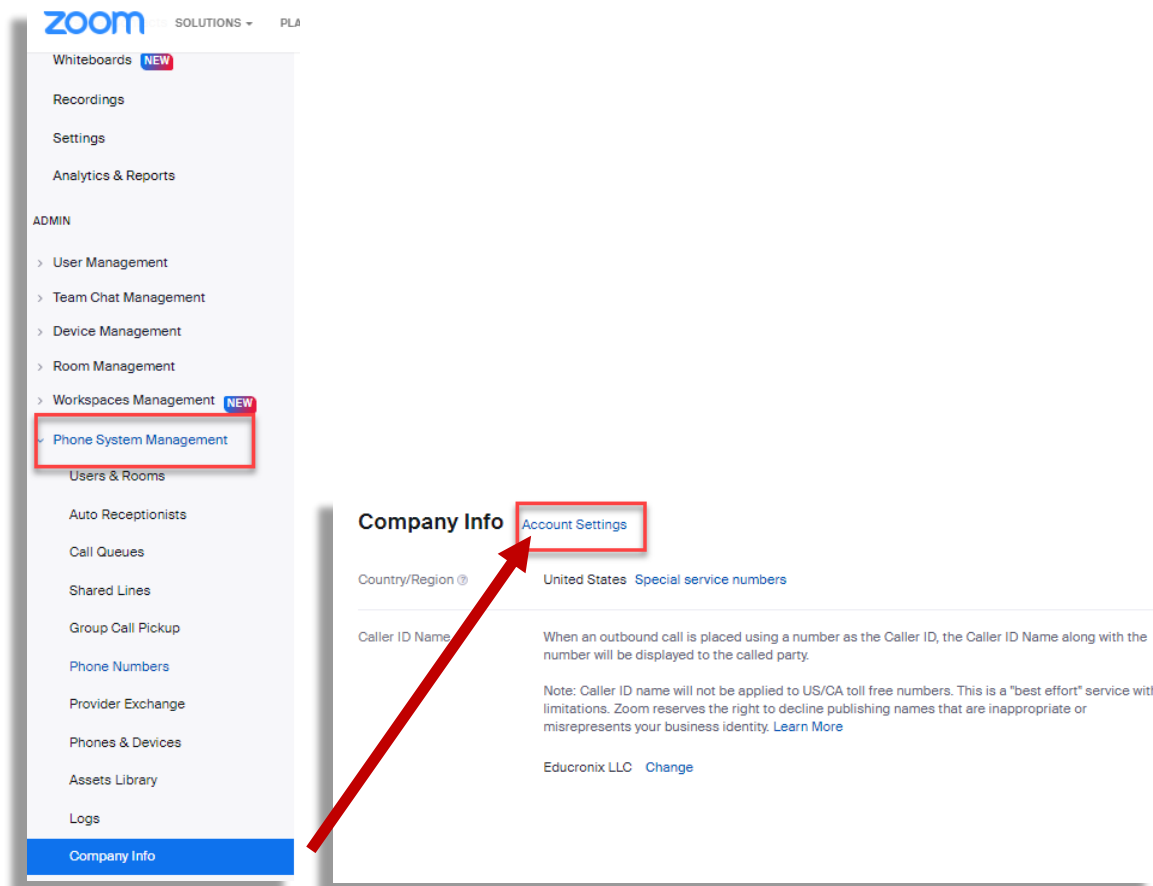
- [SIParator® reference Guide v 7.0.2](#)
- [How to Use Generic Header Manipulation](#)
- [Guidance & Installation – Ingate Software SIParator® Firewall/SIParator](#)

Zoom Phone Settings and Requirements

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

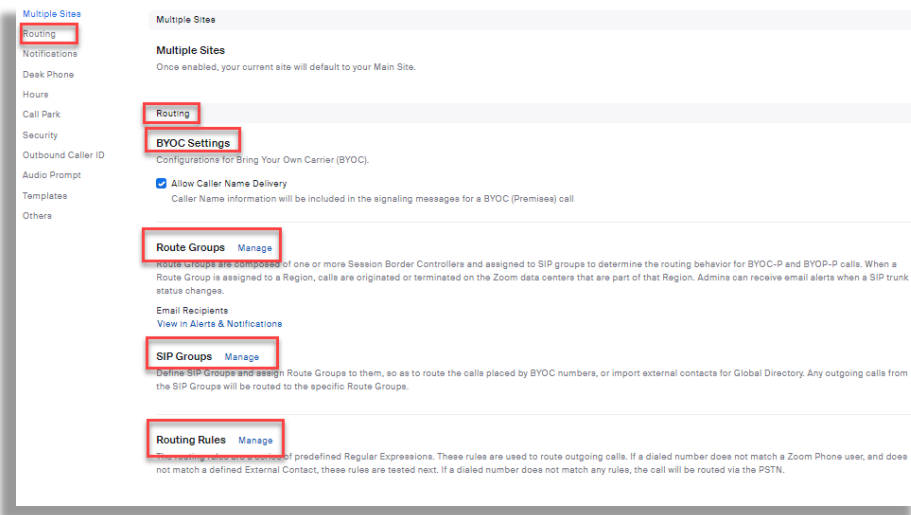
Once you have it enabled, you'll notice the following fact in your Zoom account's dashboard.

First, you'll see a Phone System Administration section:



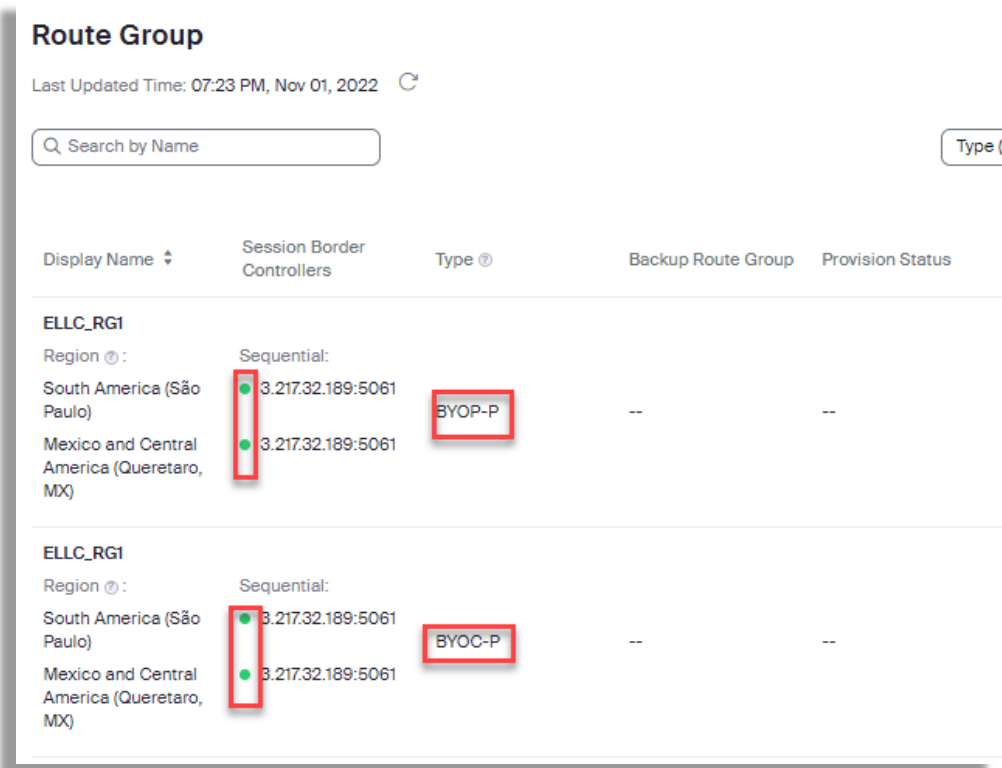
Select Company Information, and then select **Account Settings**

There are 4 important sections you should pay attention to:



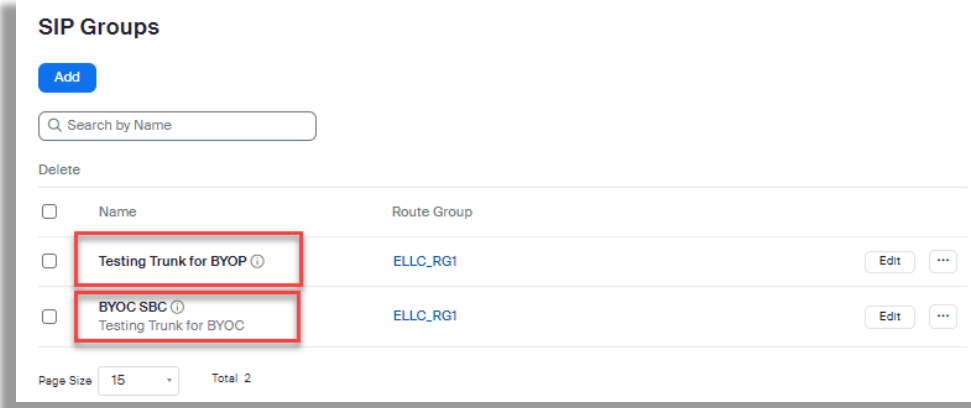
Route Groups (Manage)

You will be able to see the connection status of both services (BYOC and BYOP)



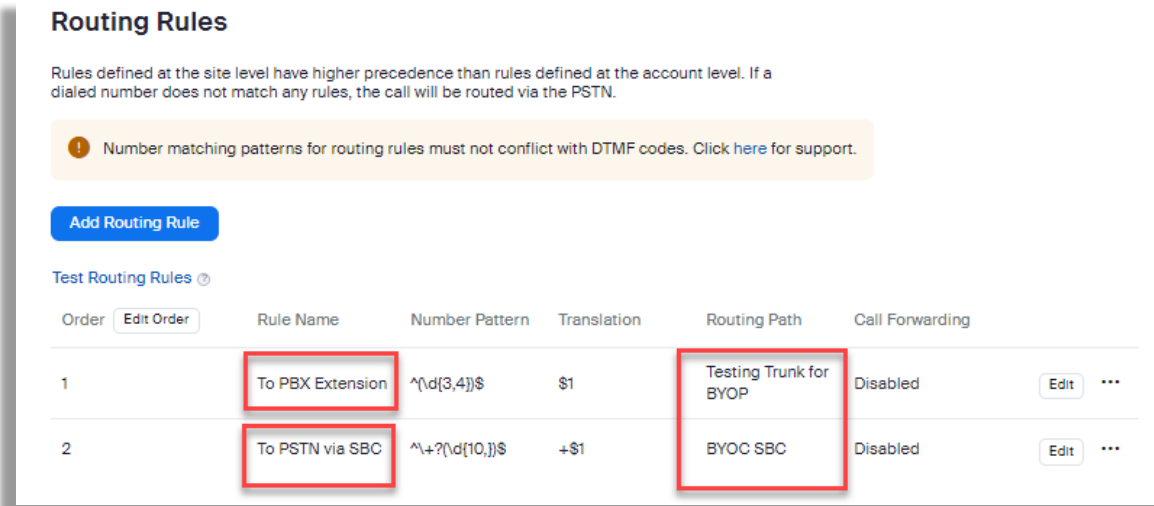
SIP Groups (Manage)

You will need to have at least one SIP group for BYOC and one for BYOP like this:



Routing Rules (Manage)

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



Declarations

SIParator® and Ingate® are trademarks of Ingate System AB

Zoom® and Zoom Phone® are trademarks of Zoom Video Communications, Inc.

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

Help and support

If you need additional information, advice or any kind of support regarding the content of this document, please contact:

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