Application Note

EDUCRONIX
TELECOMM SKILLS AT YOUR HANDS

Connecting Zoom Phone Premise Peering (BYOC & BYOP)

with Ingate SIParator® SBC

Introduction 4
  About the Zoom Phone System 4
  About Ingate SIParator® SBC product family. 4
Deployment scenarios 6
  Proof of Concept Topology 6
Configuring Zoom Phone System 7
Configuring SIParator® SBC 7
  Pre-requisites 7
  Configuring Inside and Outside Interfaces 8
  Other Network related configurations 11
  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® 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 32
  Configure Dial Plan 34
    Enabling SIP Options for Zoom requests 34
    Route outbound from Zoom to PSTN 35
    Route Outbound from PBX to PSTN 36
    Route PBX←→Zoom 37
  Configuring Transcoding 39
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.

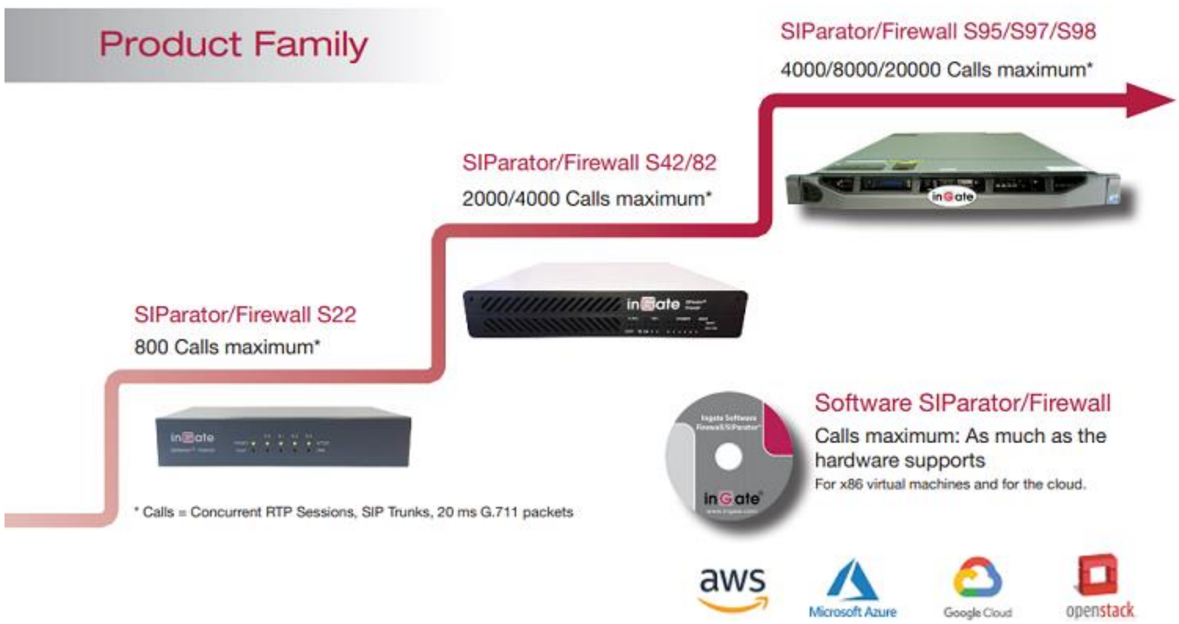
About Ingate SIParator® SBC product family.

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® SBC resolves this problem, working in tandem with your current security solutions.

The Ingate 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.

The Ingate Firewall®, 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®/Firewalls® 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® 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®/Firewall® solution to meet their needs at any given moment.

With more than 10,000 installations worldwide, the Ingate SIParator® 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® SBC and Trunking with te Zoom Phone System has been tested in the following setup.

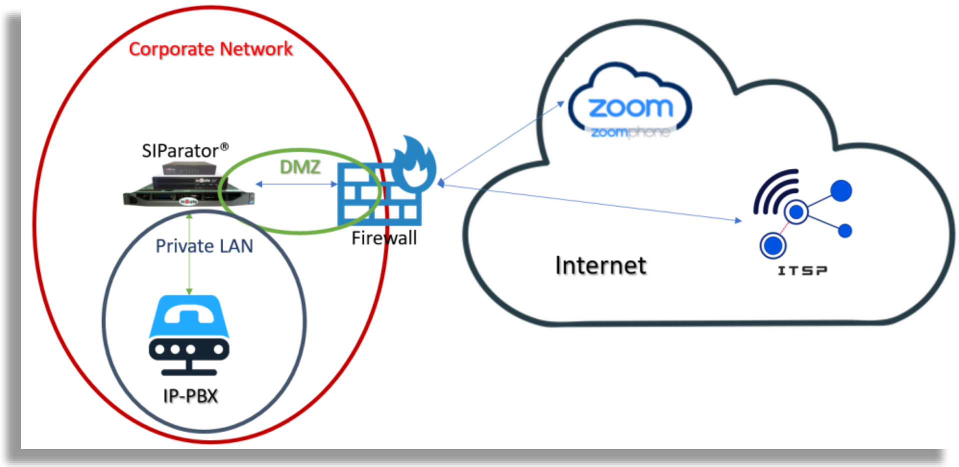


Figure 1: Deployment Layout

Configuration for SIParator® 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® SBC

Pre-requisites

For this use case, validation has been done running SIParator® 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 support@educronix.com

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® appliances according to your expected workload, or a VM properly dimensioned if you are using Software SIParator®

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® DMZ ip address.
- Public certificates issued by one of the Zoom supported Cas.

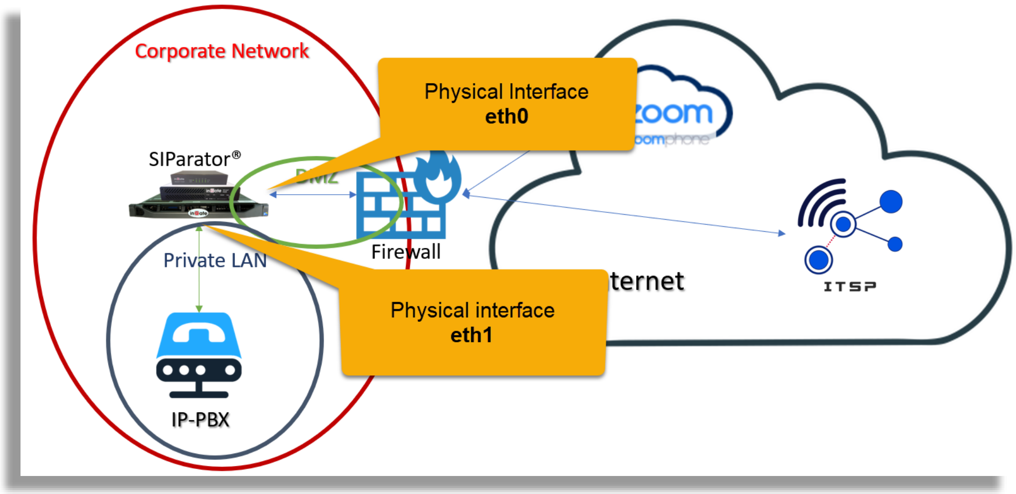
Configuring IP Network Interfaces

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® 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:

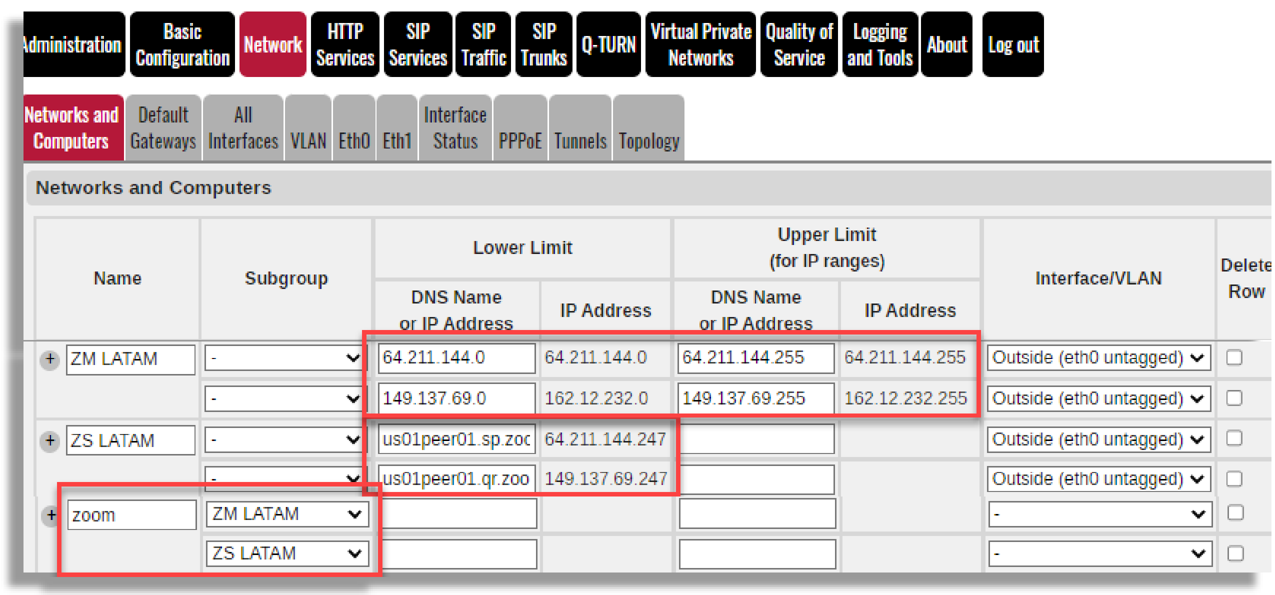
Traffic Type	Protocol	Port	Source	A Record	Destination	Region
Signaling	TCP/TLS	5061	Customer SBC	us01peer01.sc.zoom.us us01peer01.ny.zoom.us us01peer01.dv.zoom.us	162.12.233.59 162.12.232.59 162.12.235.85	North America
				us01peer01.sp.zoom.us us01peer01.qr.zoom.us	64.211.144.247 149.137.69.247	LATAM
				us01peer01.am.zoom.us us01peer01.fr.zoom.us	213.19.144.198 213.244.140.198	EMEA
				us01peer01.sy.zoom.us us01peer01.me.zoom.us	103.122.166.248 103.122.167.248	Australia
				us01peer01.sg.zoom.us us01peer01.ty.zoom.us	149.137.41.246 207.226.132.198	APAC
				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	Destination Ports	Destination IPs	Region
Media	UDP/SRTP	Customer SBC	20000-64000	162.12.232.0/22	North America
				64.211.144.0/24 149.137.69.0/24	LATAM
				213.19.144.0/24 213.244.140.0/24	EMEA
				103.122.166.0/23	Australia
				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.

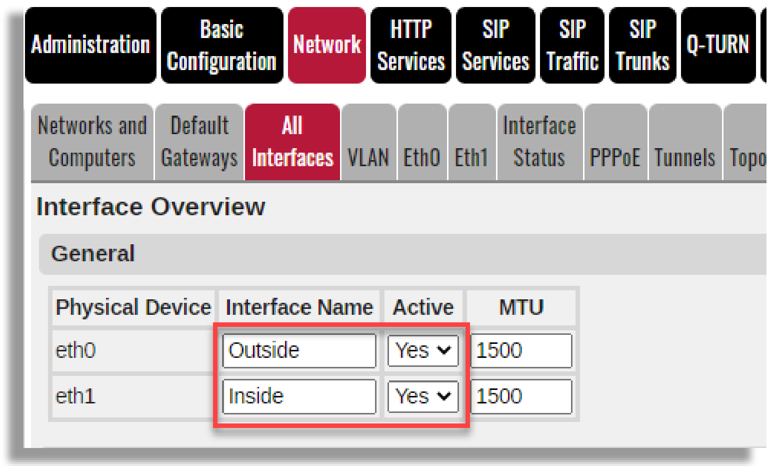
First, we will assign all those IP addresses and address ranges names to be easily used later in the configuration



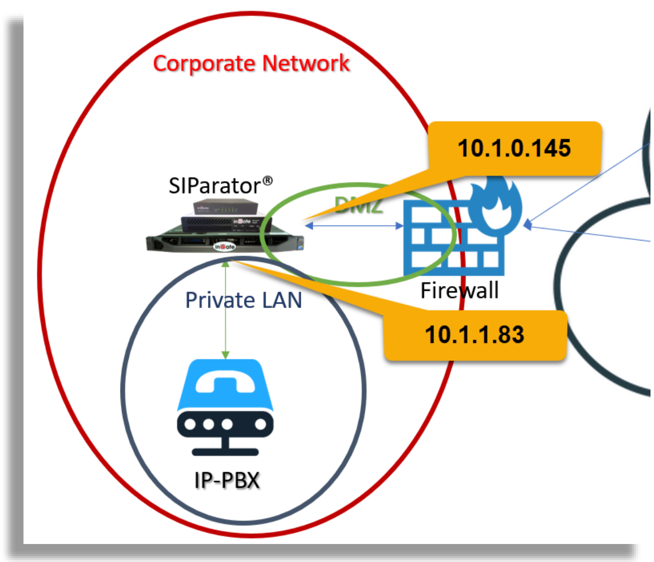
Notice:

- ZM MEDIA → Zoom Media in LATAM
- ZS LATAM → Zoom Signaling in LATAM
- zoom → 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)

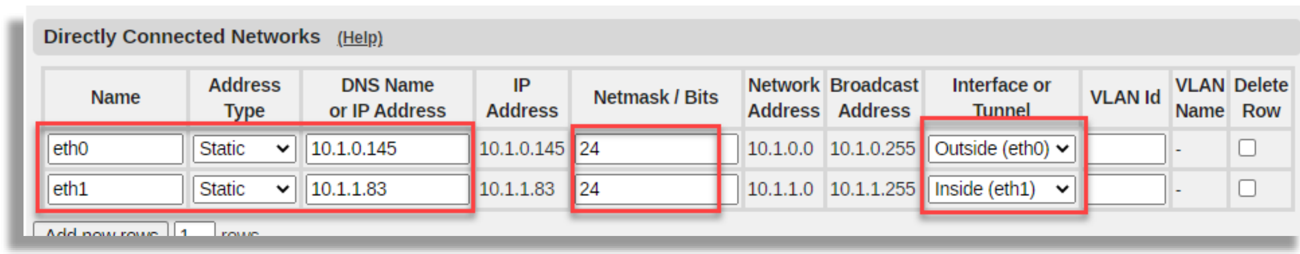


Looking at our topology:

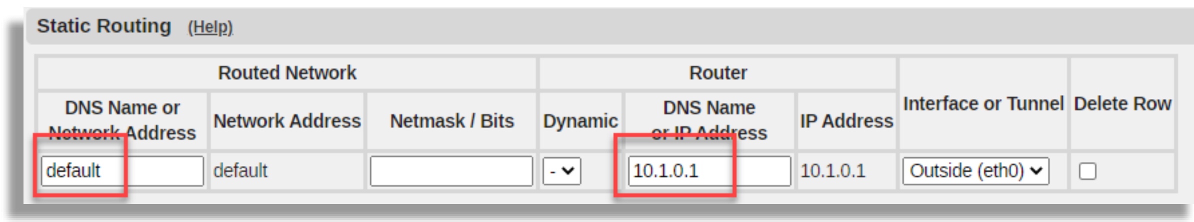


In our case,

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

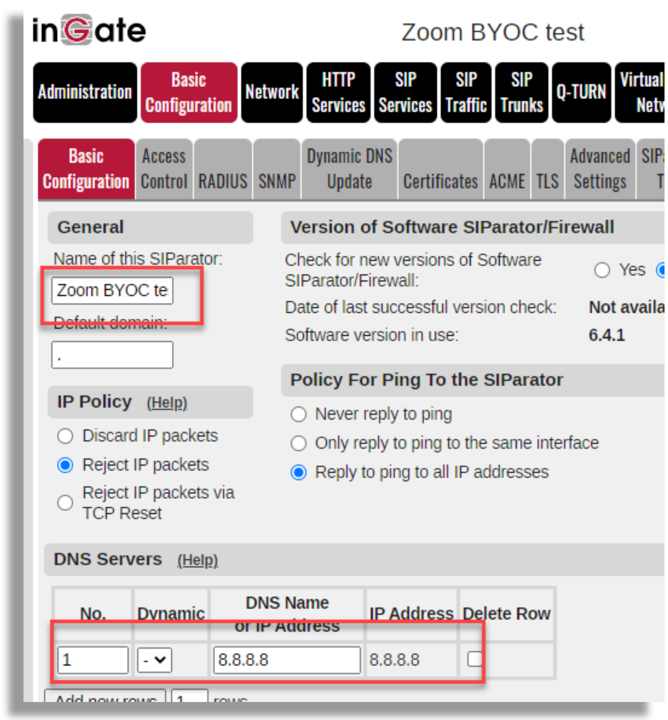


Static route for the default gateway:



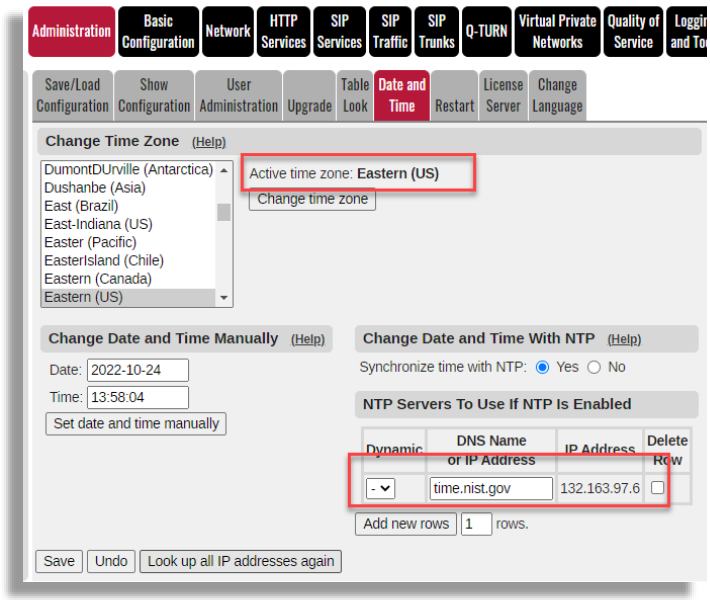
Other Network related configurations

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



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®. We are assuming to be located in EST time zone.



Configuring TLS for Zoom

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

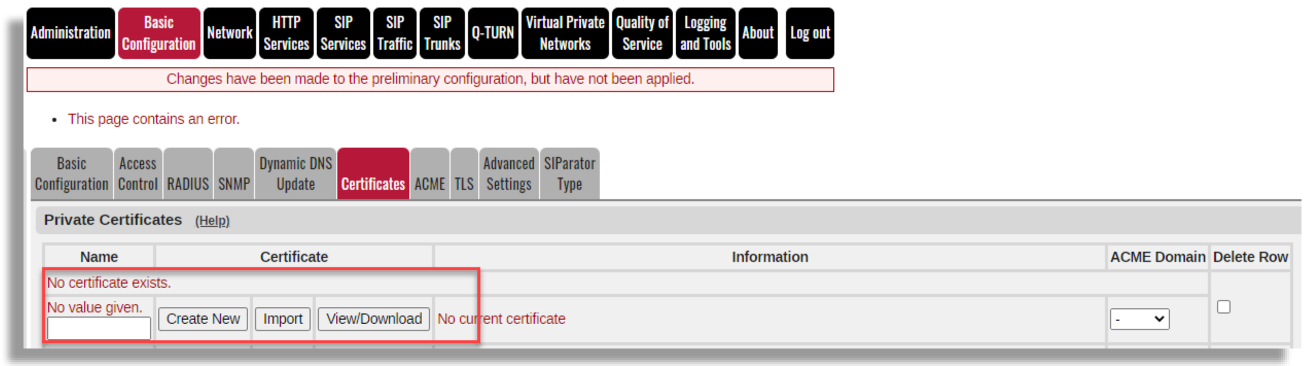
In order to enable TLS we will need appropriate public certificates. With SIParator there are two ways to acquire, install and maintain TLS certificates.

- **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®.
- **Using ACME**. Using SIParator built in ACME client and use the appropriate ACME enabled Authority in compliance with Zoom accepted CAs.

Using CSR

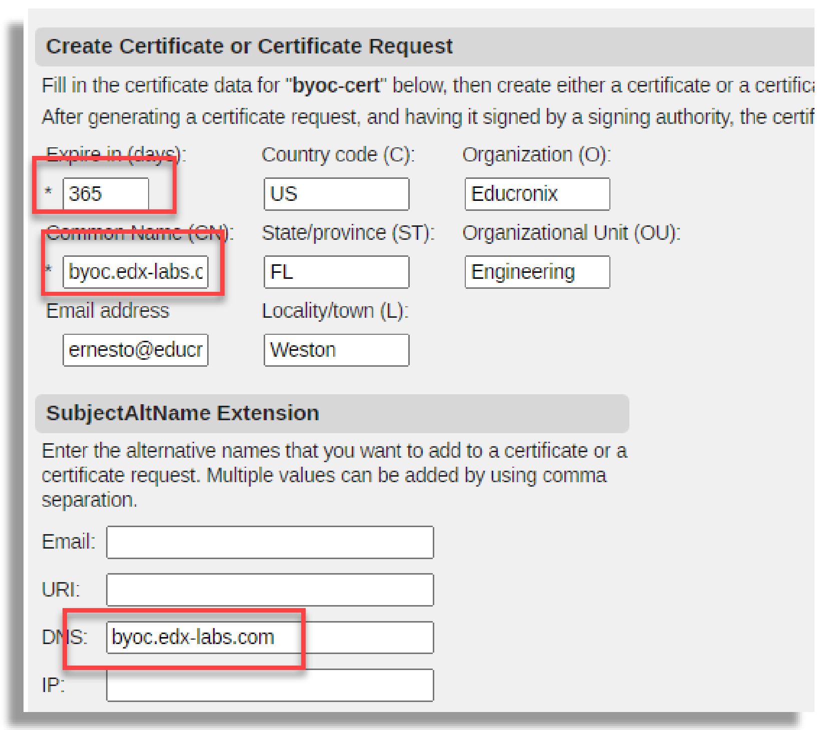
First, we will need to create a CSR (Certificate Signature Request).

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



Assign a name and click on "Create New"

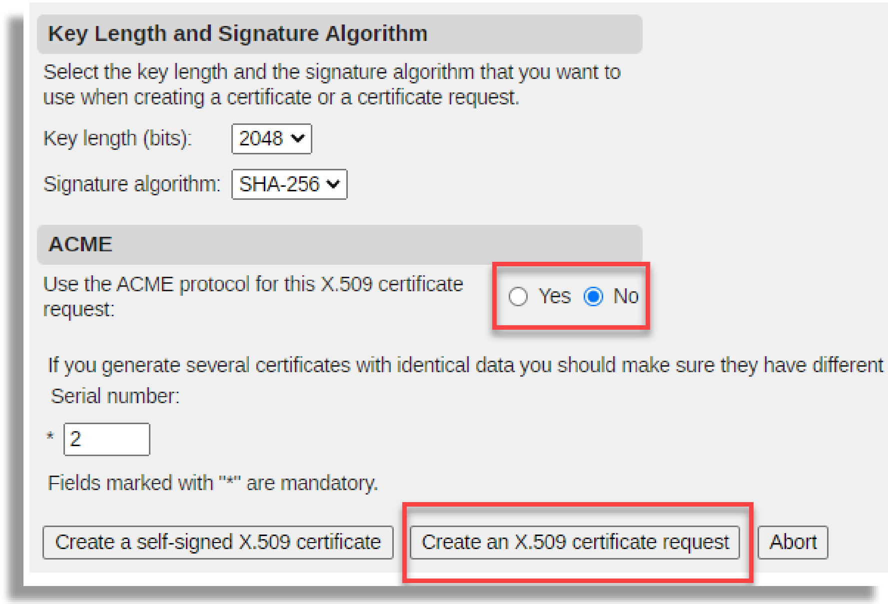
Fill the Information requested and make sure the Common Name and SubjectAltName extension DNS points to the SIParator FQDN that resolves on the Public IP address associated to the outside interface:



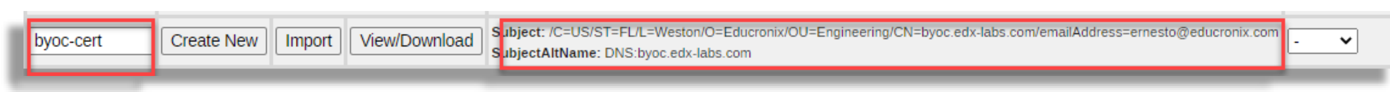
Notice Expire in (days) and Common Name (CN) are mandatory fields.

All remaining fields can be left on default values.

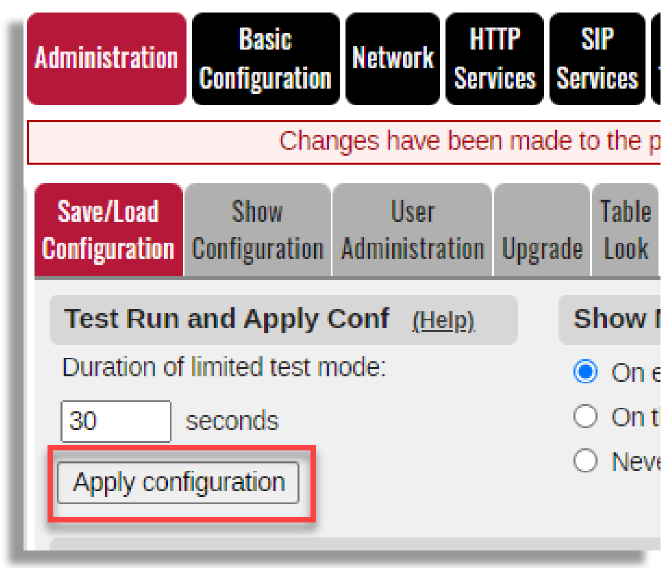
Click on "Create an X.509 certificate request"



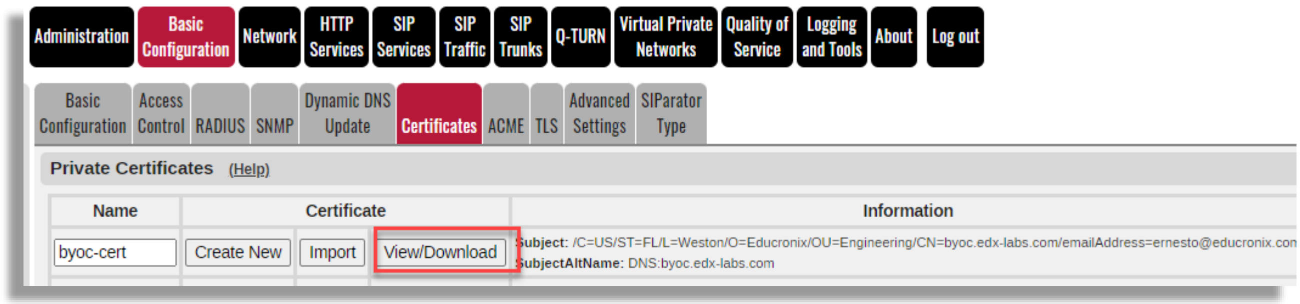
Certificate request will show like this:



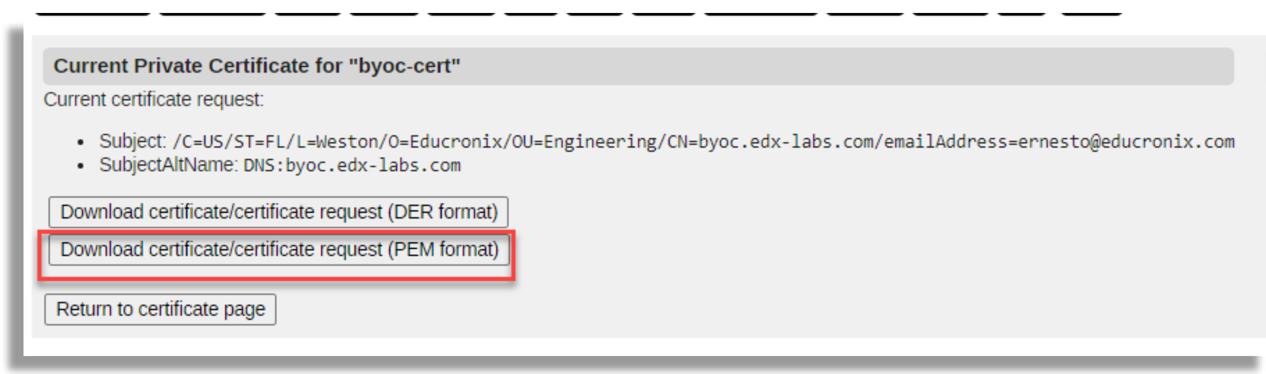
Apply changes



Go back to the certificate and Click on “View/Download”



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.



Downloaded file should look like this:

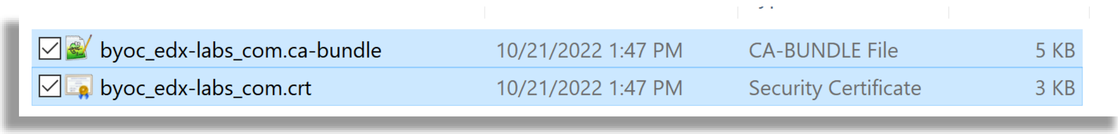

-----BEGIN CERTIFICATE REQUEST-----
MIIDDCCAfQCAQAwgZcxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJGTDEPMA0GA1UE
kAI2B3mQyjS2J4Ac65G548HEhmIkGx94oIhjq60Kgx47aDYQVQV263OYq6+8NV35
s7b+UOfjqGsz7+m/g/PZiw6Rvh2fVM2V+Uuj5d9j3TTweRjhb7V325NEmdw/SXCr
SO6K0CZWyl5sr5mv6FQUNw==
-----END CERTIFICATE REQUEST-----

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

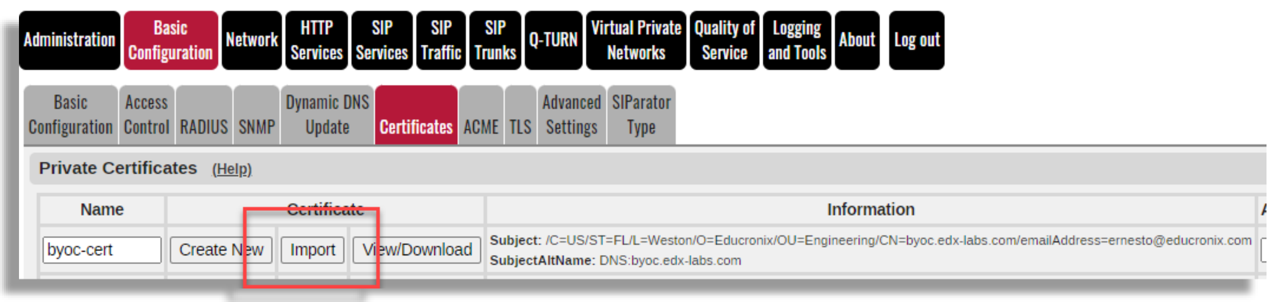
Once signed they will provide you with a set of files, usually 2:

- Signed Certificate
- Intermediary Bundle Certificates.

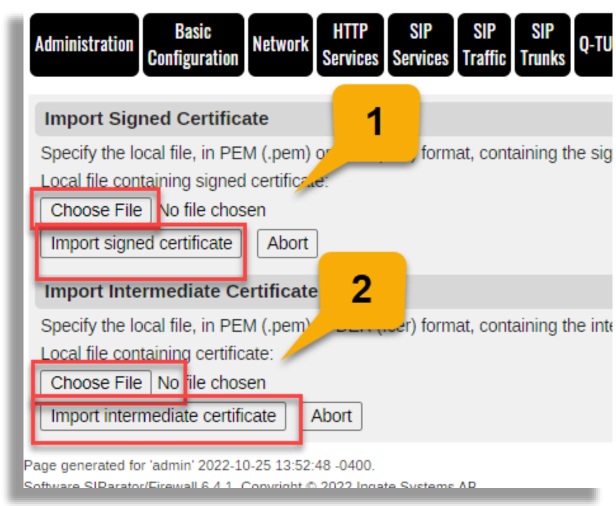
Similar to this:



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

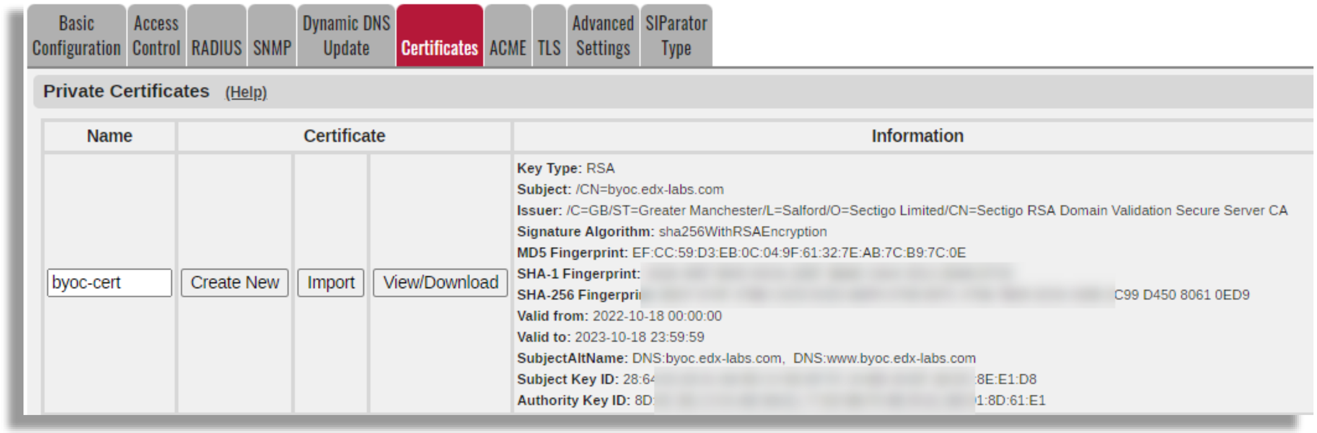


First import the certificate, save and apply and then load the bundle.



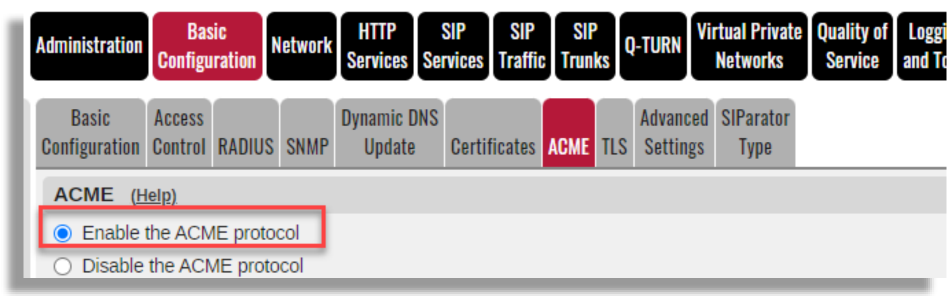
Save and apply the changes again.

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



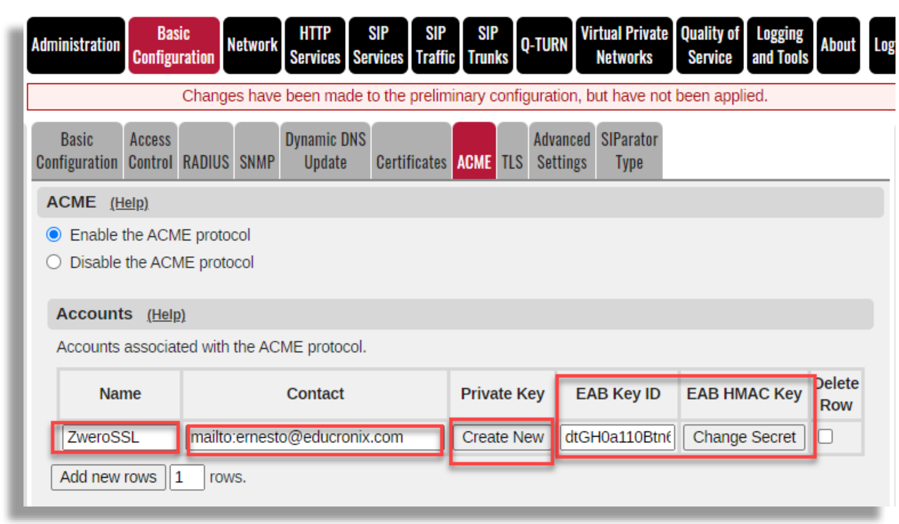
Using ACME

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



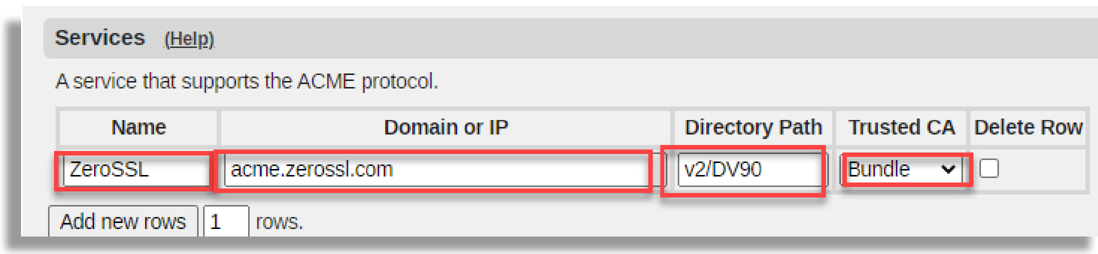
For the purpose of this document, we have selected one Certification Authority supporting ACME protocol that complies with Zoom requirements.

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



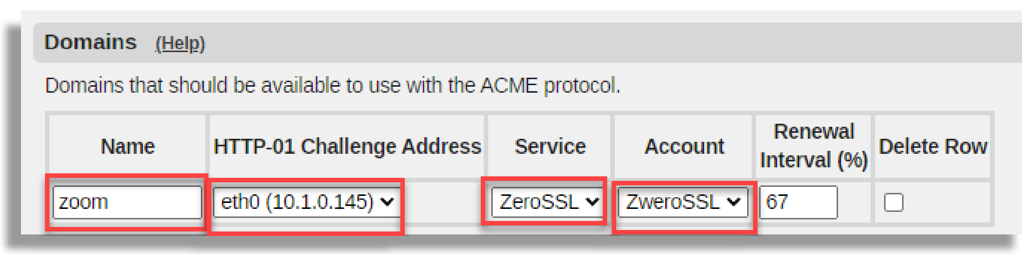
- Assign Name
- Add contact information with the format mailto:xxxxx@yyyy.zzz to provide who will be receiving updates and notifications from the CA.
- Generate a "Private Key" by pressing "Create New"
- Add EAB Key ID and EAB HMAC Key provided by the CA (for ZeroSSL, it can be found in the Developers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

Add the service



- 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.

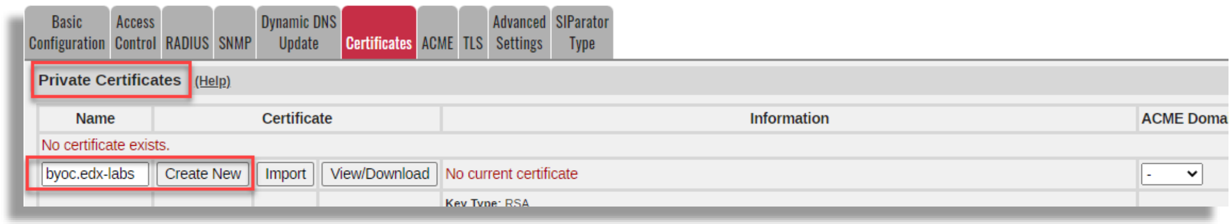


- Assign a Name
- Select the interface that will be facing the outside (Internet)
- Select the Service and Account (previously created).
- Keep the default value of 67% to establish when the request for renewal will be triggered

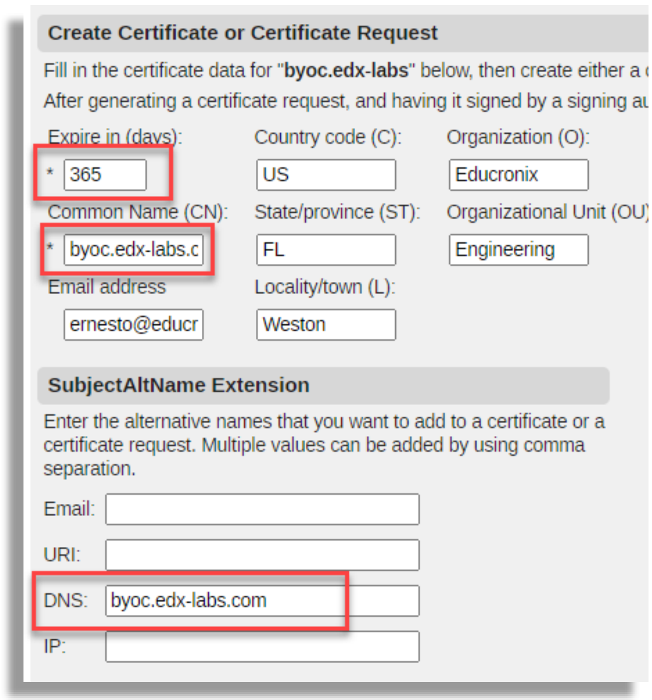
Now we are ready to create the Certificate using ACME.

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":

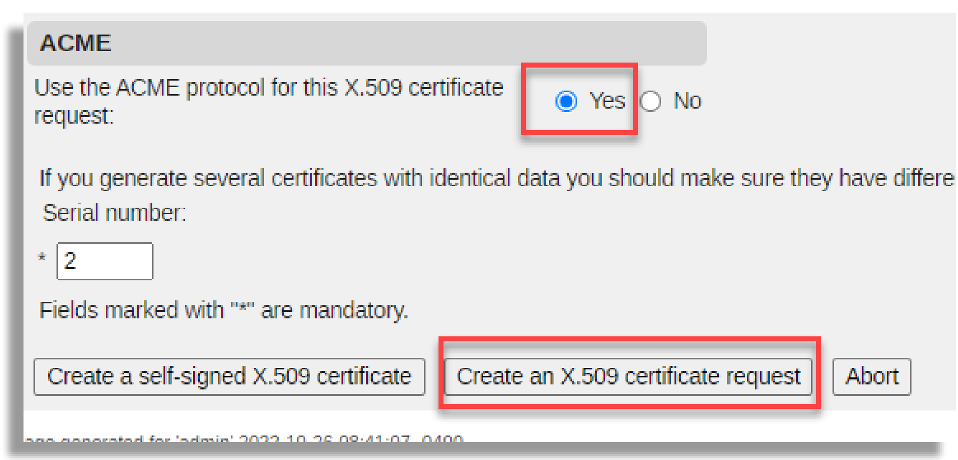


Complete the information here:



Notice:

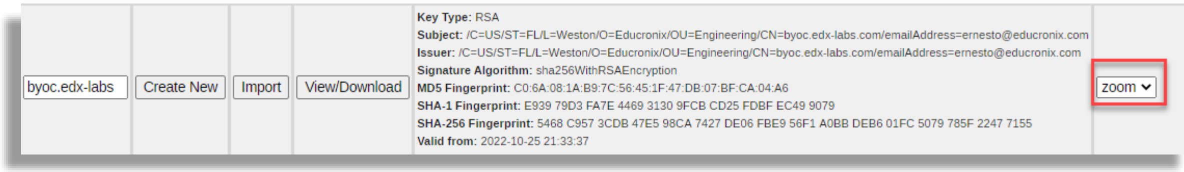
- Expire and Common name are mandatory fields, however, Expire will be defined by the Certification Authority regardless of the value you enter.
- Common Name and DNS must match the FQDN associated with the SIParator® public IP.



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

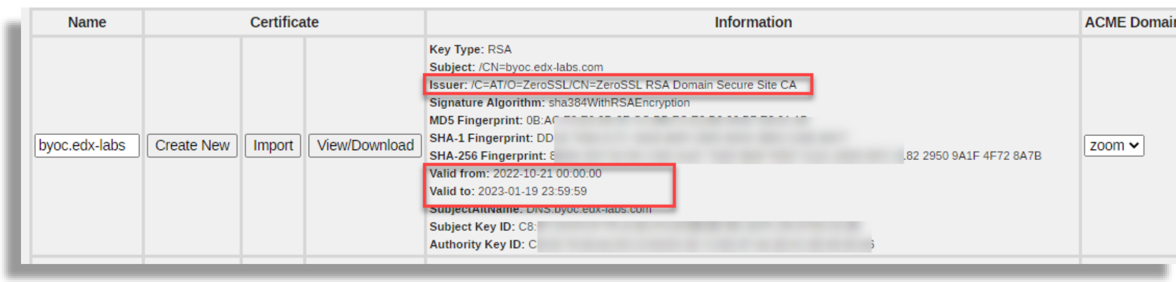
This creates a temporary self signed certificate until the CA provides the new signed certificate.

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



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.



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 support@educronix.com

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® Basic Configuration.

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

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

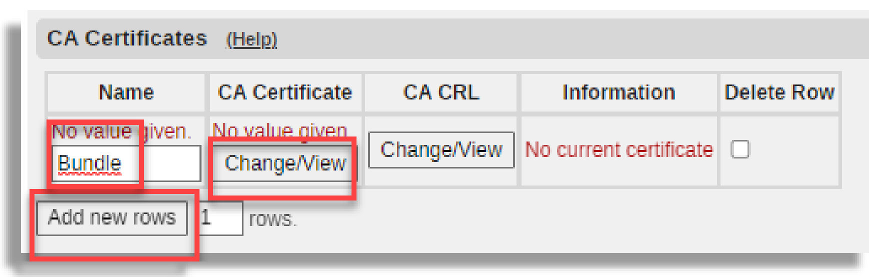
https://cacerts.digicert.com/DigiCertGlobalRootCA.crt.pem

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

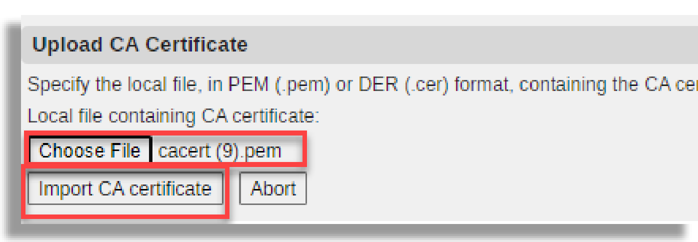
https://cacerts.digicert.com/DigiCertGlobalRootG3.crt.pem

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

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

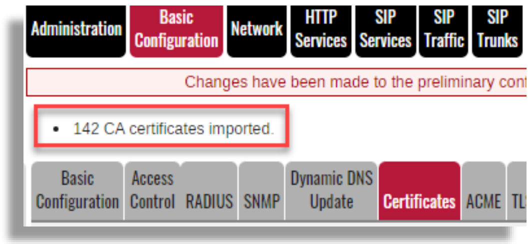


- Assign a name (Bundle in our case)
- Click on CA Certificate "Change/View"



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

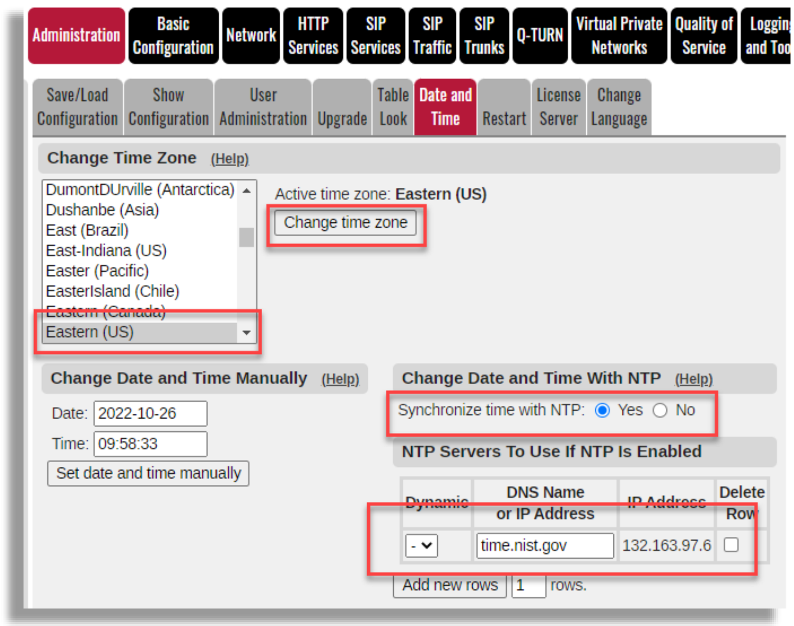
In the case of the Bundle, you will see about 142 certificates loaded under the same name.



Apply and Save your changes.

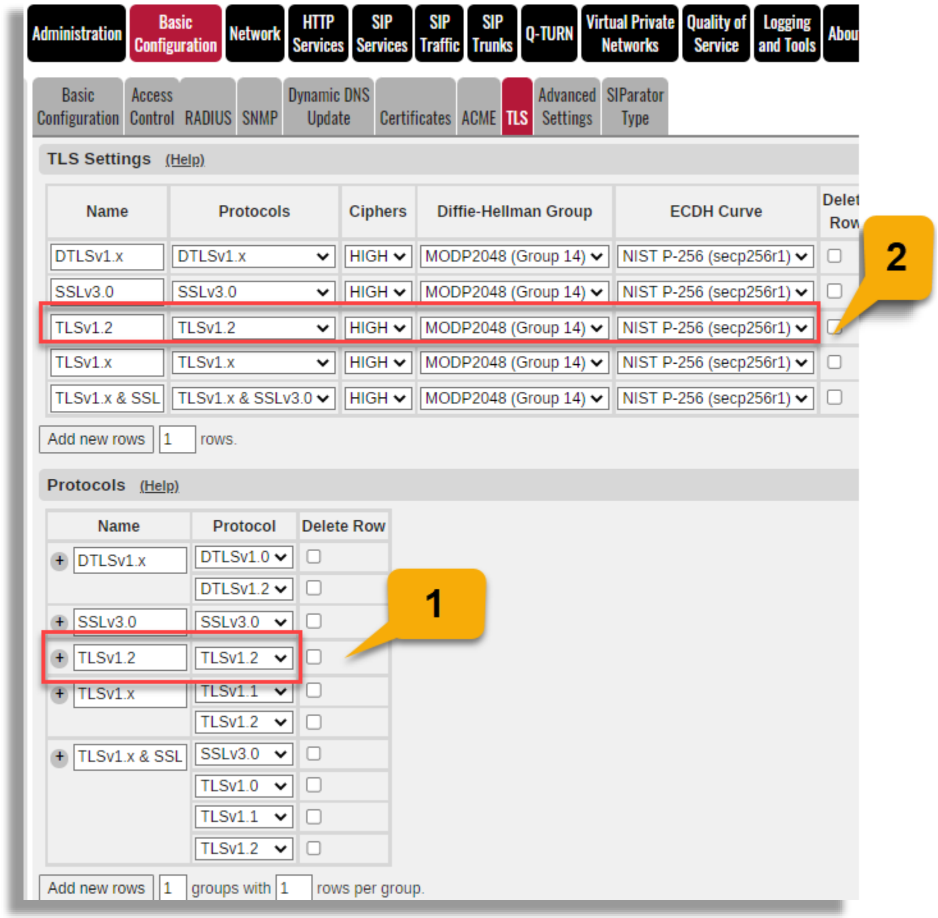
Configure NTP Server

To have SIParator® 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.

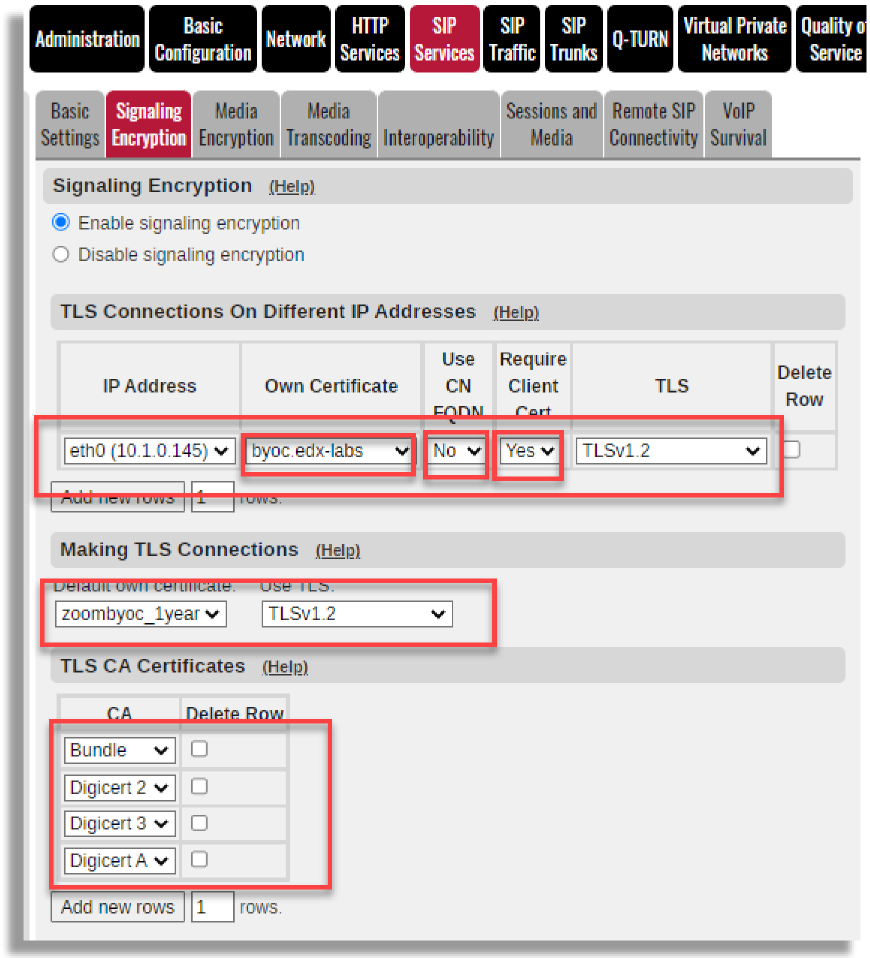


- Add a new entry in the Protocols section which includes only TLSv1.2, we named it "TLSv1.2
- Save, and then add a new entry in TLS Settings table as shown in the picture above. We also named it "TLSv1.2"

Configuring SIP in SIParator®

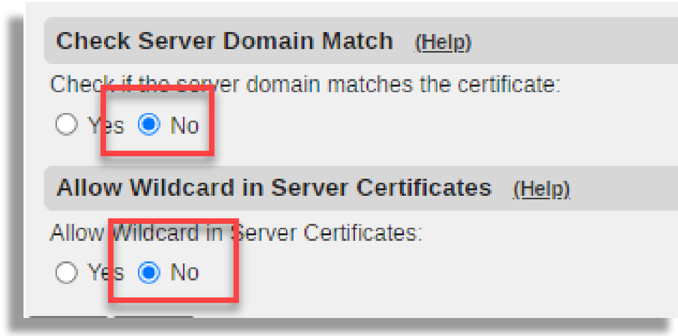
Now we will setup all signaling related configuration for SIP.

Setup TLS signaling



- 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® (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.

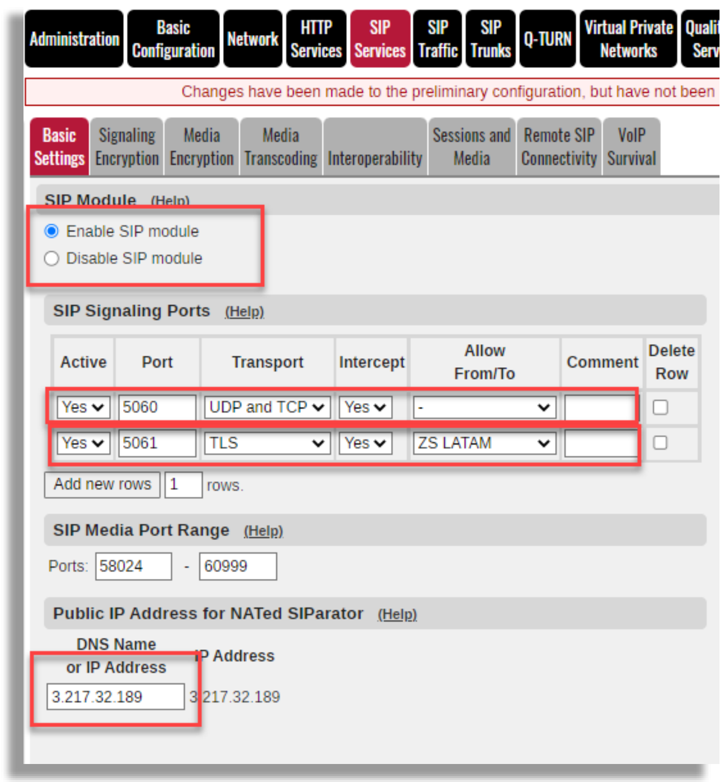
You will also leave the next two setting in "No" as shown here:



Setup SIP Ports

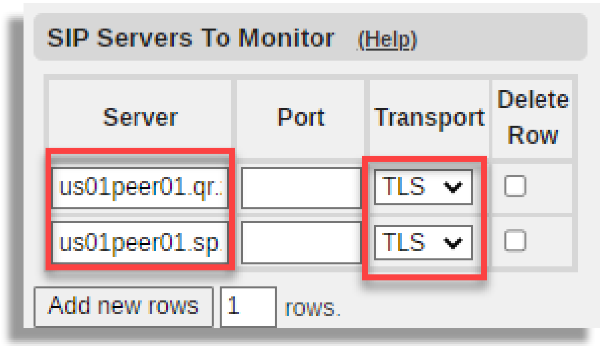
Now we will need to associate ports to be used for SIP (UPD/TCP and/or TLS)

Go under SIP Services → 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® 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® will monitor those IP's by sending periodically SIP OPTIONS.



We are monitoring then:

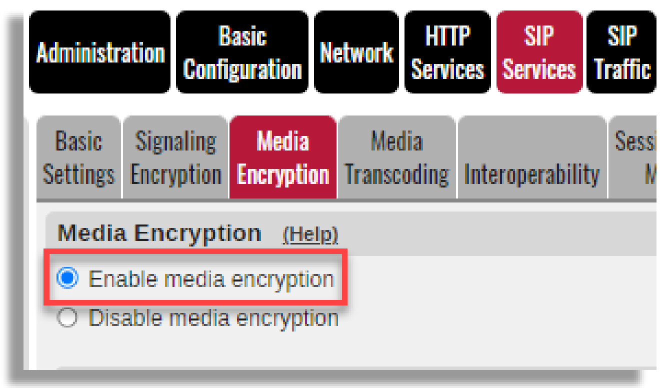
- us01peer01.qr.zoom.us (Latam – México)
- us01peer01.sp.zoom.us (Latam – Sao Paulo)

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.

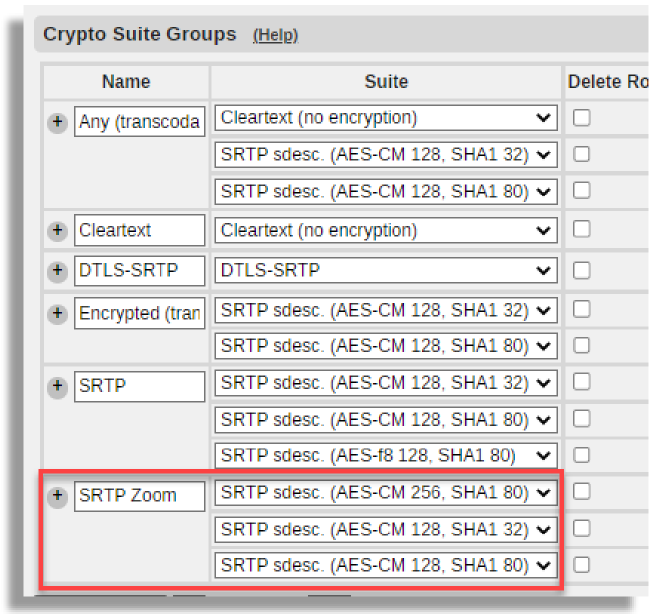
Configure Media Encryption

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

To configure Media Encryption, make sure it is enabled:

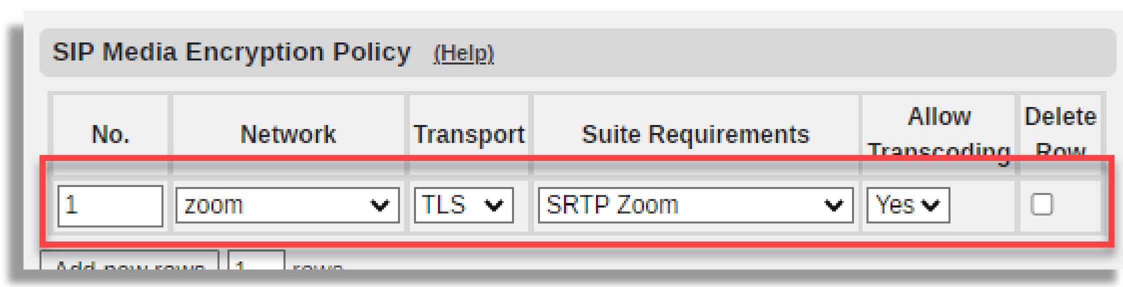


Then we will create a Crypto Suite Group specifically for Zoom



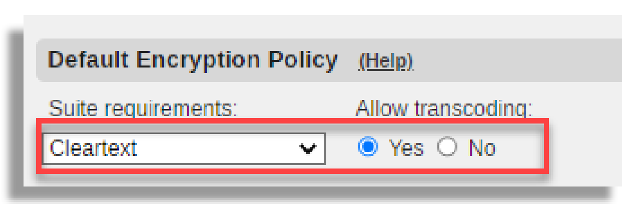
- Add one row with 3 sub-rows
- Select each sub-row associated to the suites shown in the picture

Add a Media Encryption Policy:



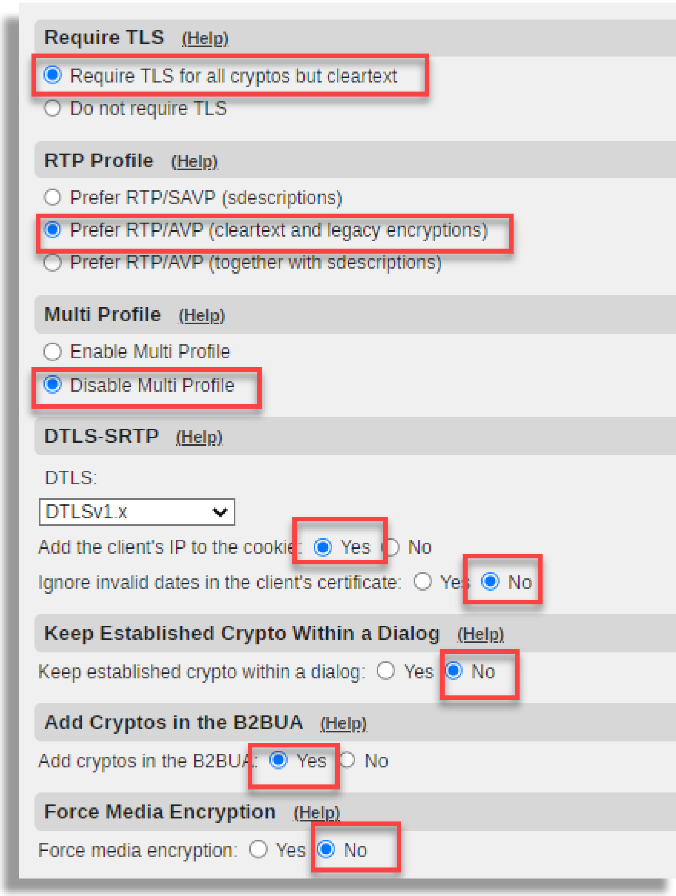
- Add a new row
- Select the aggregated network named “zoom”
- Select TLS for transport protocol
- Associate the recently created suite named “SRTP Zoom”
- Enable “Allow Transcoding”

Define a default encryption policy for anything else:



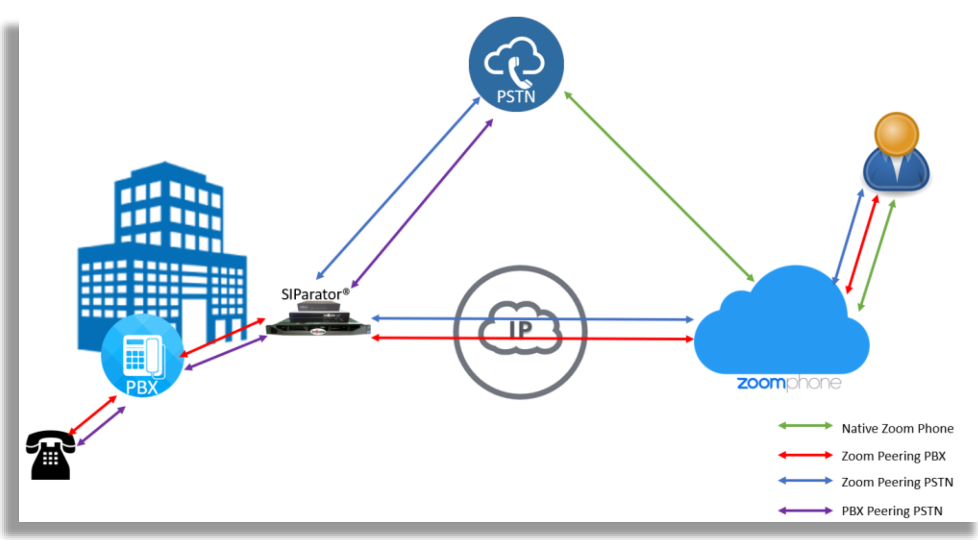
- Select “Cleartext” as the default policy (Cleartext means “No Encryption”)
- Allow Transcoding

Set the remaining parameters as shown:



Configure SIP Trunking

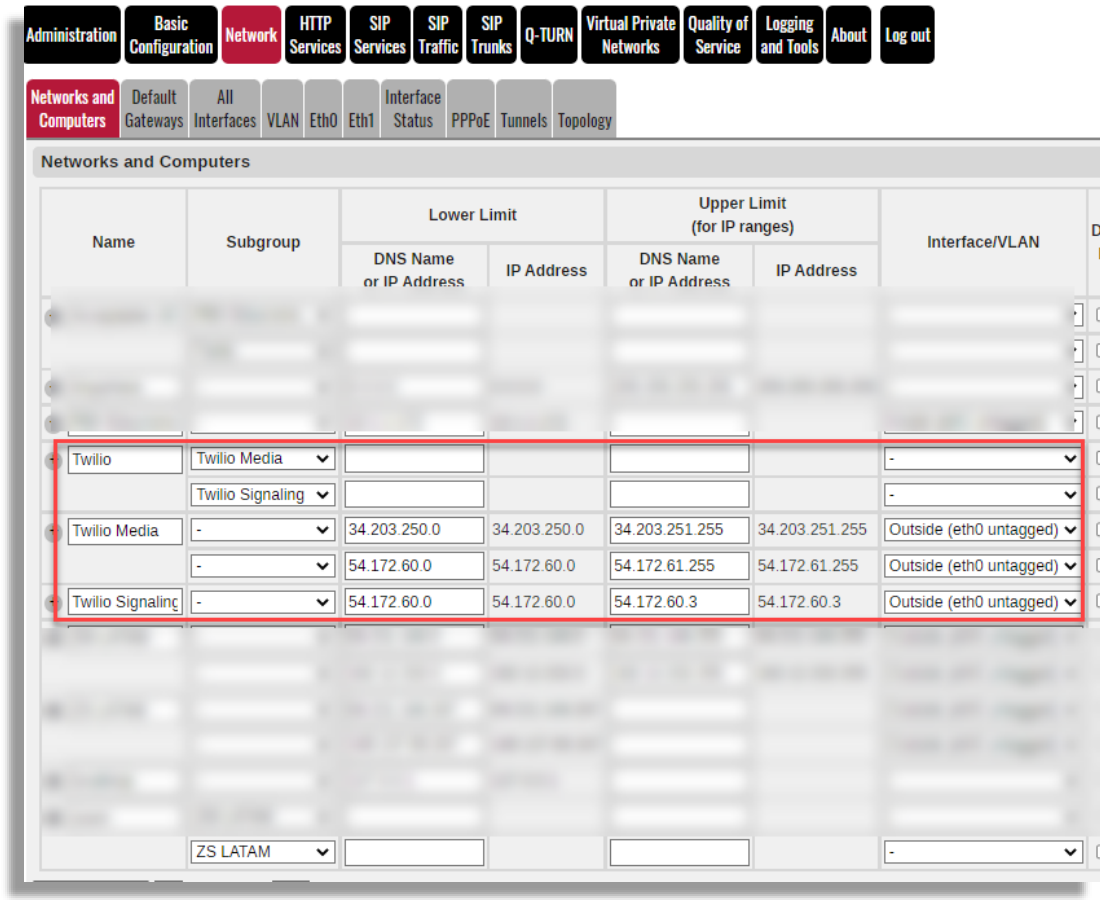
Let's understand how SIP flows looks like in our case:



Setting up Zoom-PSTN Trunk Group

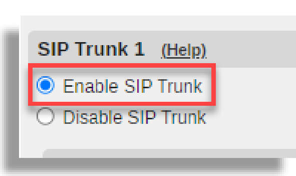
In our case we are using Twilio SIP Trunking Service for demonstration purposes.

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



Let's setup the Trunk Group

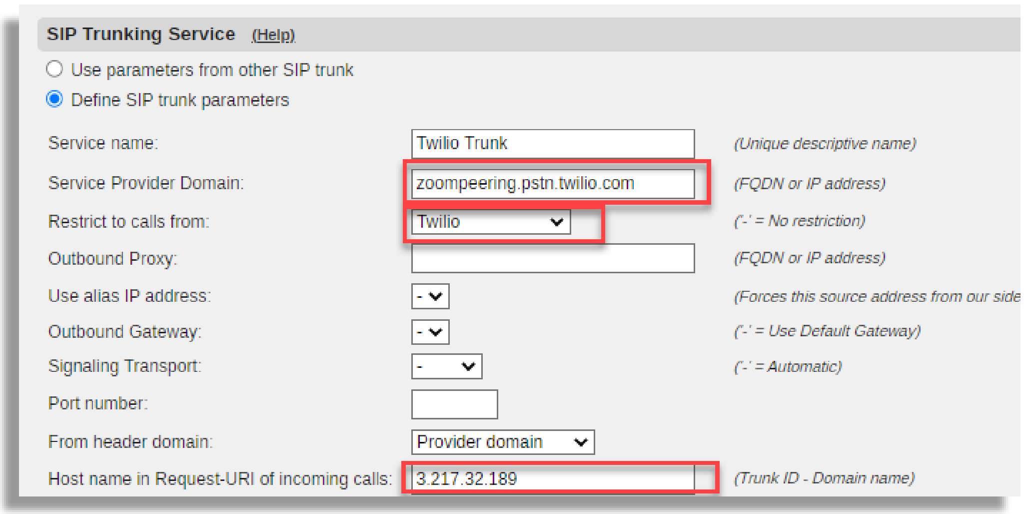
First, we will enable a new Trunk Group by enabling from the pull-down options:



Click on “Goto SIP Trunk page” and Enable the Trunk Group

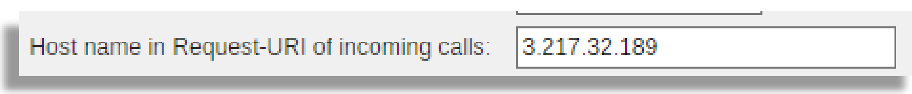
We are using Twilio Elastic SIP Trunk Service and have as assigned FQDN: **zoompeering.pstn.twilio.com**

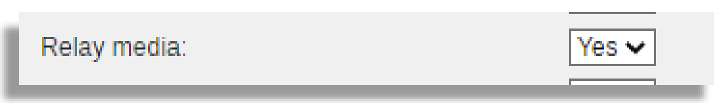
Lest define the trunk:



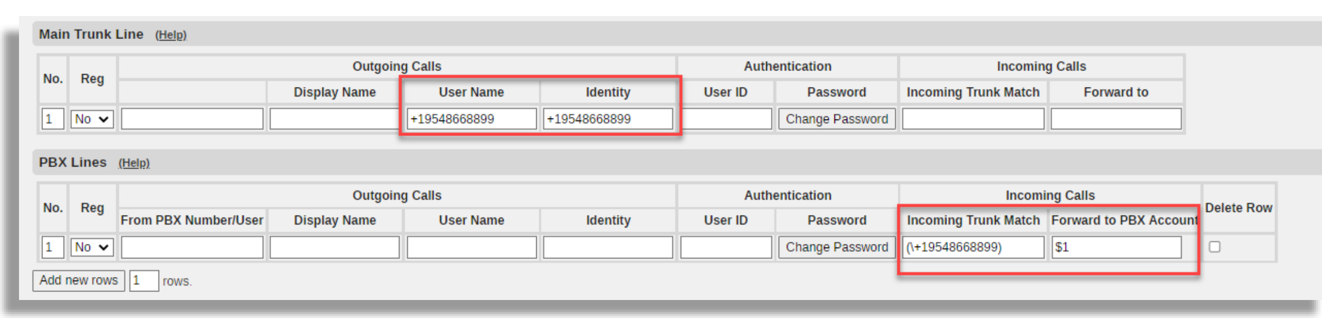
- Assign a name to the trunk group
- Use the provided Proxy FQDN as the Service Provider Domain.
- As our SIParator® is behind a firewall (DMZ) we will need to enter the public IP in the Host Name in Request-URI.

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



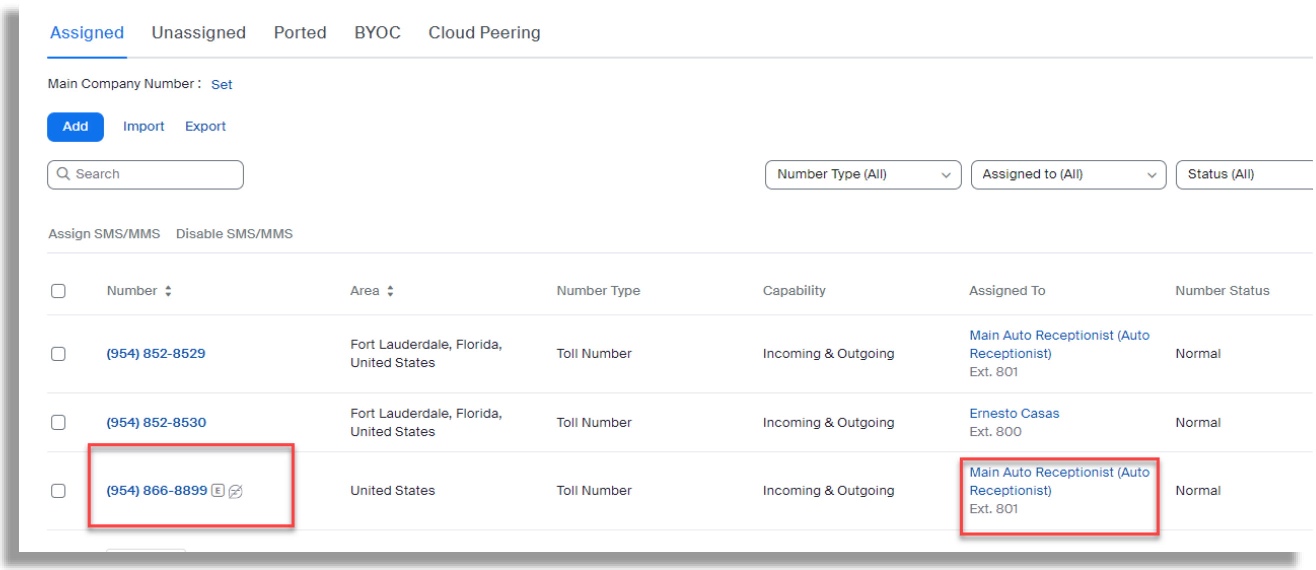


Now we will setup the Matching rules to route inbound DID’s designated for Zoom users or auto attendant:



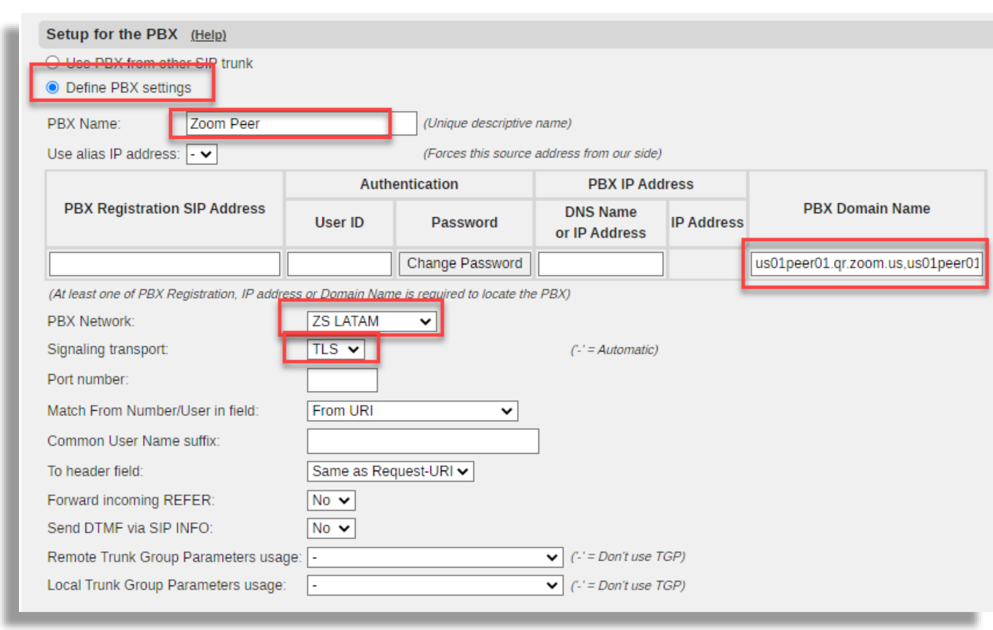
If you have more than one DID, you can keep adding rows to the PBX Lines table and match additional DID's. You can also use regular Expression for Matching.

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.



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 ",".



- Select "Define PBX Settings

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

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

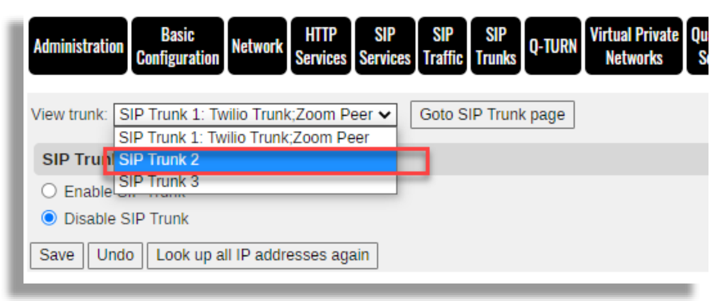
Traffic Type	Protocol	Port	Source	A Record	Destination	Region
Signaling	TCP/TLS	5061	Customer SBC	us01peer01.sc.zoom.us us01peer01.ny.zoom.us us01peer01.dv.zoom.us	162.12.233.59 162.12.232.59 162.12.235.85	North America
				us01peer01.sp.zoom.us us01peer01.qr.zoom.us	64.211.144.247 149.137.69.247	LATAM
				us01peer01.am.zoom.us us01peer01.fr.zoom.us	213.19.144.198 213.244.140.198	EMEA
				us01peer01.sy.zoom.us us01peer01.me.zoom.us	103.122.166.248 103.122.167.248	Australia
				us01peer01.sg.zoom.us us01peer01.ty.zoom.us	149.137.41.246 207.226.132.198	APAC
				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

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

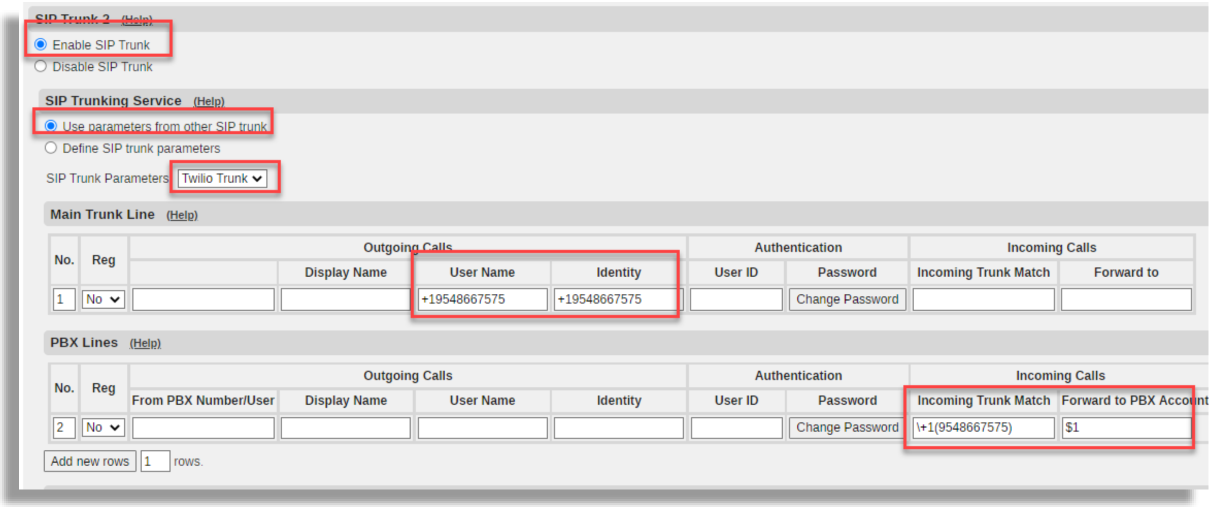
Setting up PBX-PSTN Trunk Group

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® to manage PSTN traffic for Zoom users as well as your existing PBX.

We will need to add a new Trunk Group page

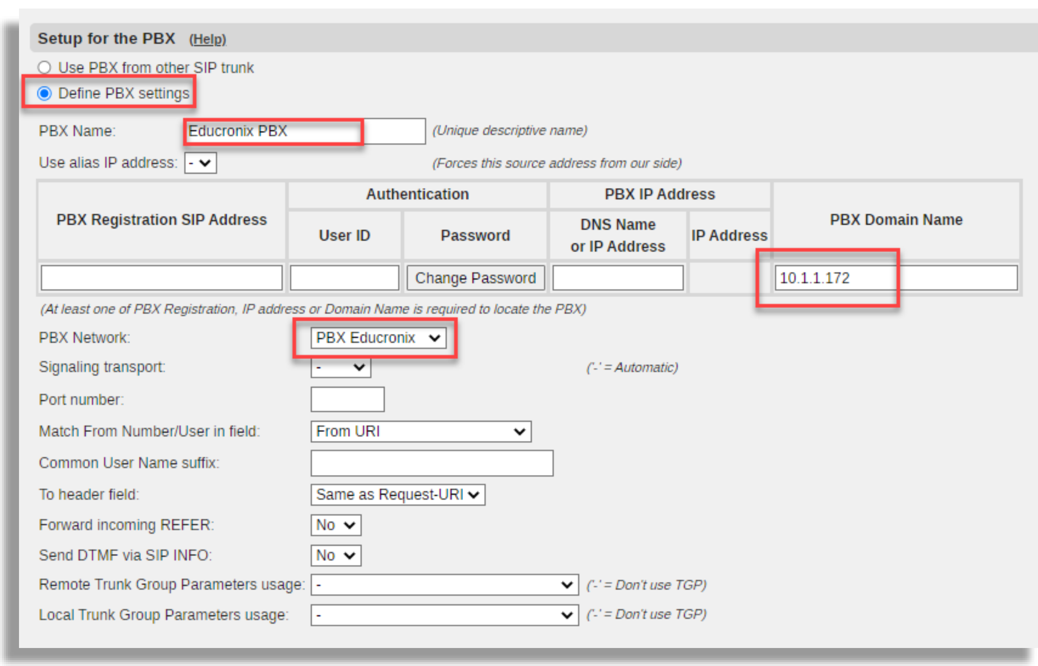


Enable Tunk Group and select "Use parameters from other SIP Trunk". This way we will use the same Trunk we already configured in the previous section.



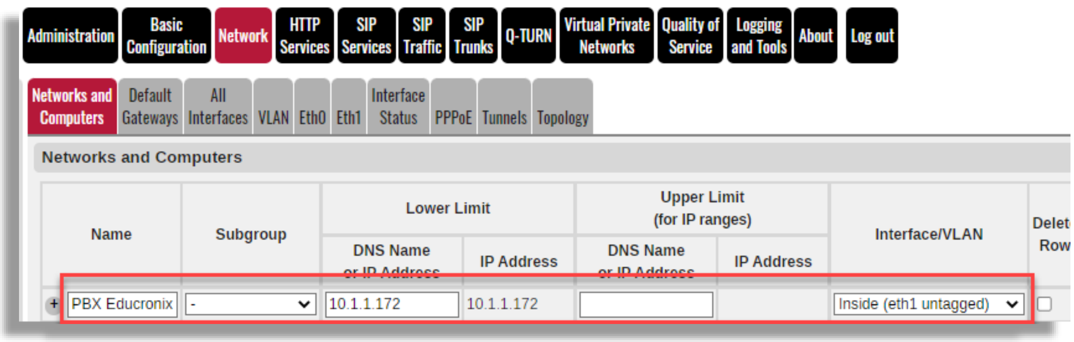
- Enable The Trunk
- Use parameters from other SIP trunk and chose Twilio Trunk (configured in the previous section)
- Wi will use a different DID and will add it to the outgoing User Name and Identity for Caller ID purposes.
- For incoming call will match the DID assigned to PBX Trunking. If you have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

Now we will setup the PBX connectivity



- 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:

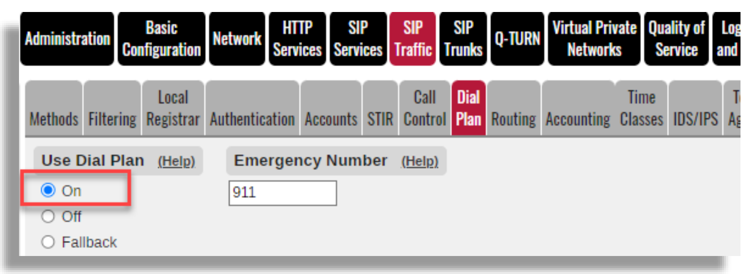


- Leave the remaining fields with the default values.

Configure Dial Plan

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

First you'll need to enable Dial Plan.



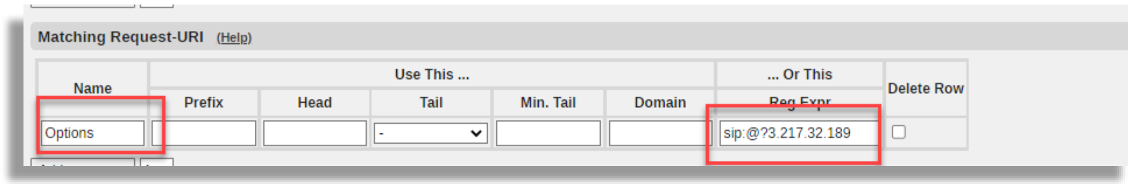
Enabling SIP Options for Zoom requests

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:

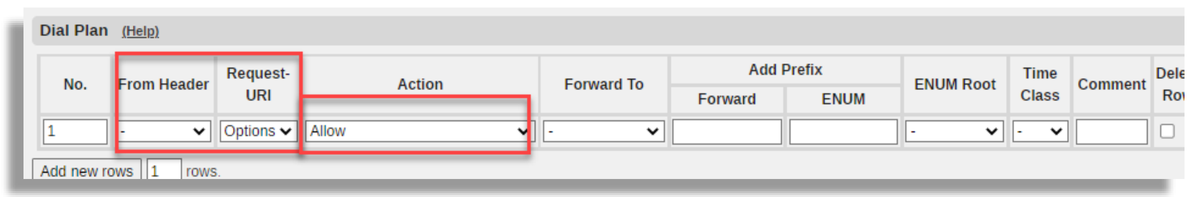
sip:@?3.217.32.189

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



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

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

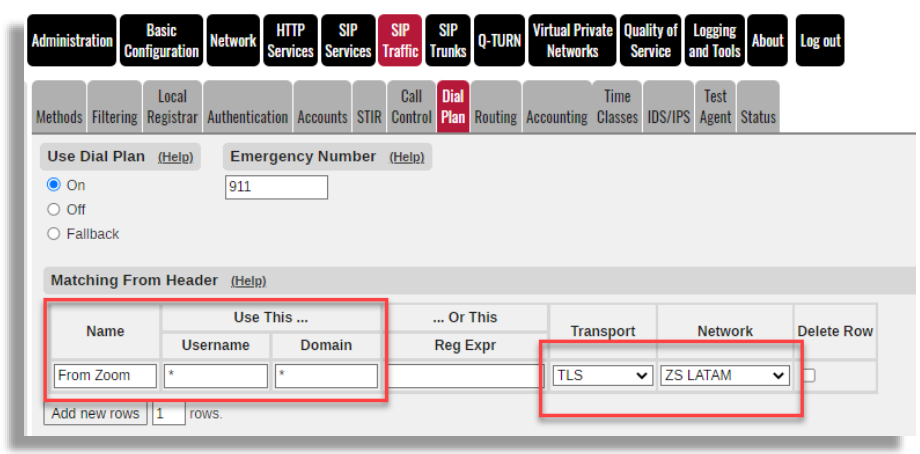


We will use then the Dial Plan for 3 main purposes:

- 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

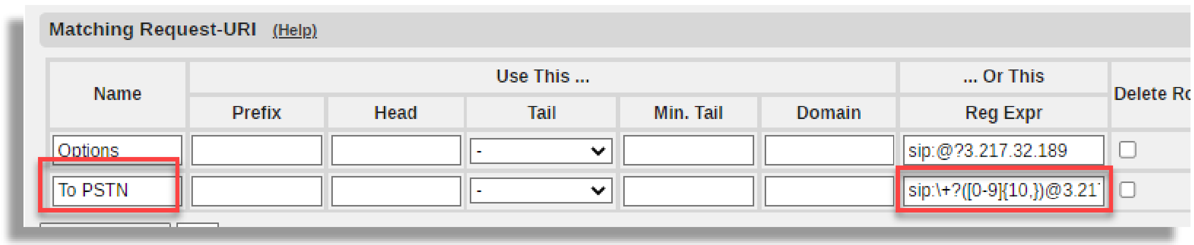
To detect/match traffic coming from Zoom we will add a rule in the match From header section



- 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)

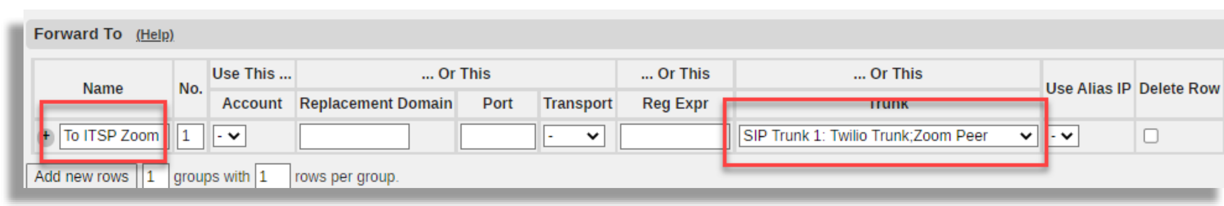
- Select the network from which the traffic will be coming from (Zoom Signaling sources)

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



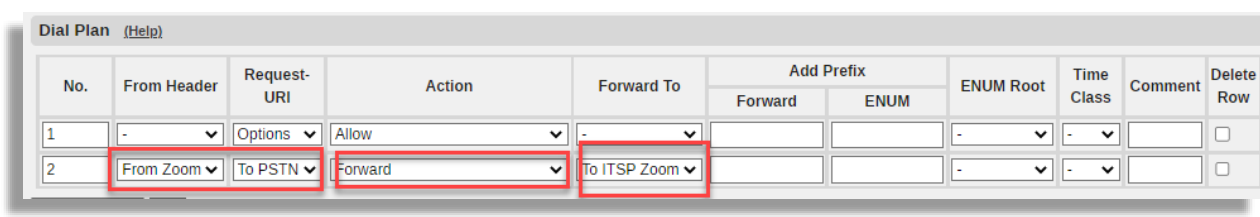
- Add a new row in “Matching Request-URI”
- Assign a name to the new rule
- Match SIP requests to an E164 number **sip:\+([0-9]{10,0}@<SIParator public ip address>**

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



- 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.



- 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.

Forward To (Help)

Name	No.	Use This ...	... Or This			... Or This	... Or This	Use Alias IP
		Account	Replacement Domain	Port	Transport	Reg Expr	Trunk	
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:

Dial Plan (Help)

No.	From Header	Request-URI	Action	Forward To	Add Prefix		ENUM Root	Time Class	Comment
					Forward	ENUM			
1	-	Options	Allow	-			-	-	
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 ←→ 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® from the PBX, or matching to a 3 or 4 digit number arriving to SIParator® from Zoom.

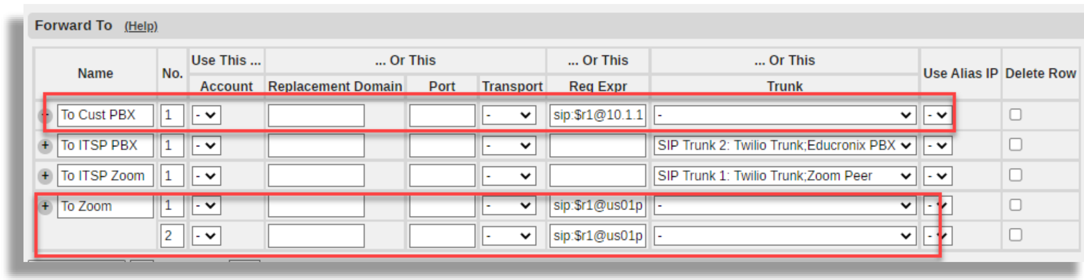
Matching Request-URI (Help)

Name	Use This ...					... Or This	Delete Row
	Prefix	Head	Tail	Min. Tail	Domain	Reg Expr	
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®.
- 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®.
- 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.

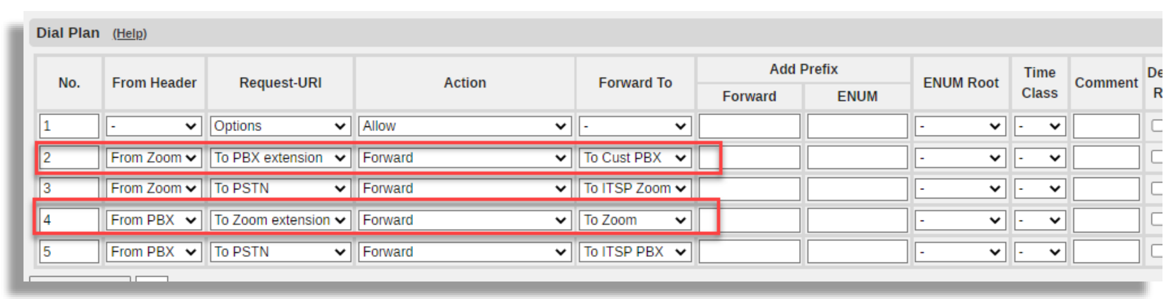


Forward To (Help)

Name	No.	Use This ... Account	... Or This Replacement Domain	Port	Transport	... Or This Req Expr	... Or This Trunk	Use Alias IP	Delete Row
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	-	-	☐
	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:$r1@<PBX IP Address>
- Add “;transport=udp;b2buawm” at the end of the expression.
- Add a New row and a sub-row to define the 2 destinations associated to LATAM Zoom Region signaling FQDNs. User Regex to define each one:
    - ***sip:$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



Dial Plan (Help)

No.	From Header	Request-URI	Action	Forward To	Add Prefix Forward	Add Prefix ENUM	ENUM Root	Time Class	Comment	De R
1	-	Options	Allow	-			-	-		☐
2	From Zoom	To PBX extension	Forward	To Cust PBX			-	-		☐
3	From Zoom	To PSTN	Forward	To ITSP Zoom			-	-		☐
4	From PBX	To Zoom extension	Forward	To Zoom			-	-		☐
5	From PBX	To PSTN	Forward	To ITSP PBX			-	-		☐

- 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)

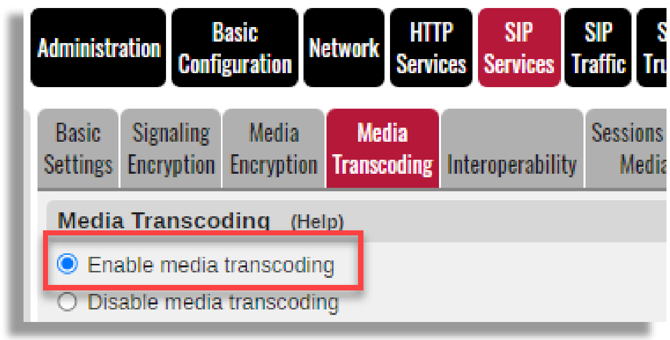
Configuring Transcoding

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

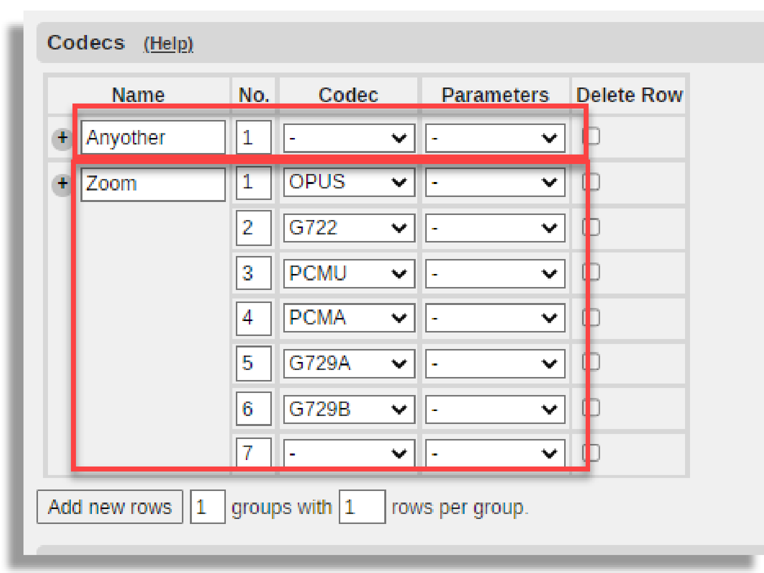
- OPUS
- G.722
- G.711A-law/µ-law
- G.729

SIParator® has software-based transcoding built-in with no extra licensing requirement.

You'll need to enable Transcoding:



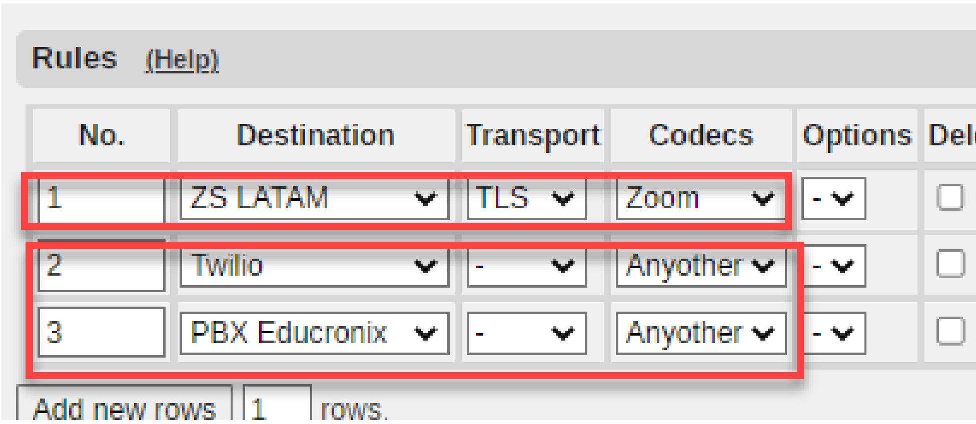
We will first create the codec groups needed:



- 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.

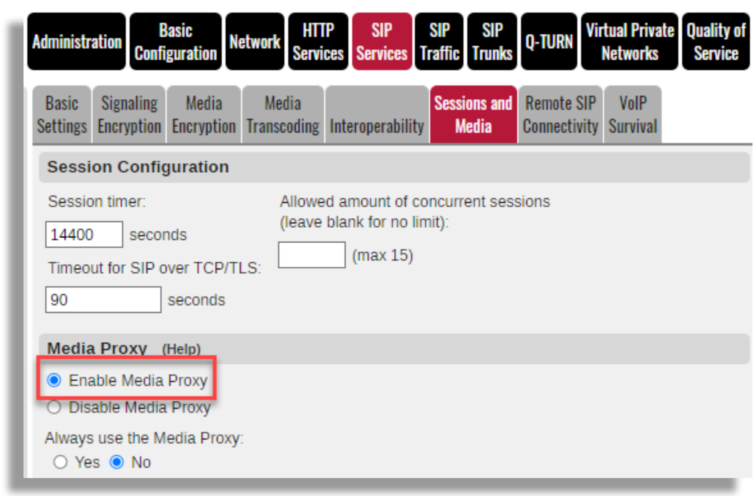
- Second Row, named Zoom, with have one sub-row per each Zoom supported Codec as mentioned before

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



- 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

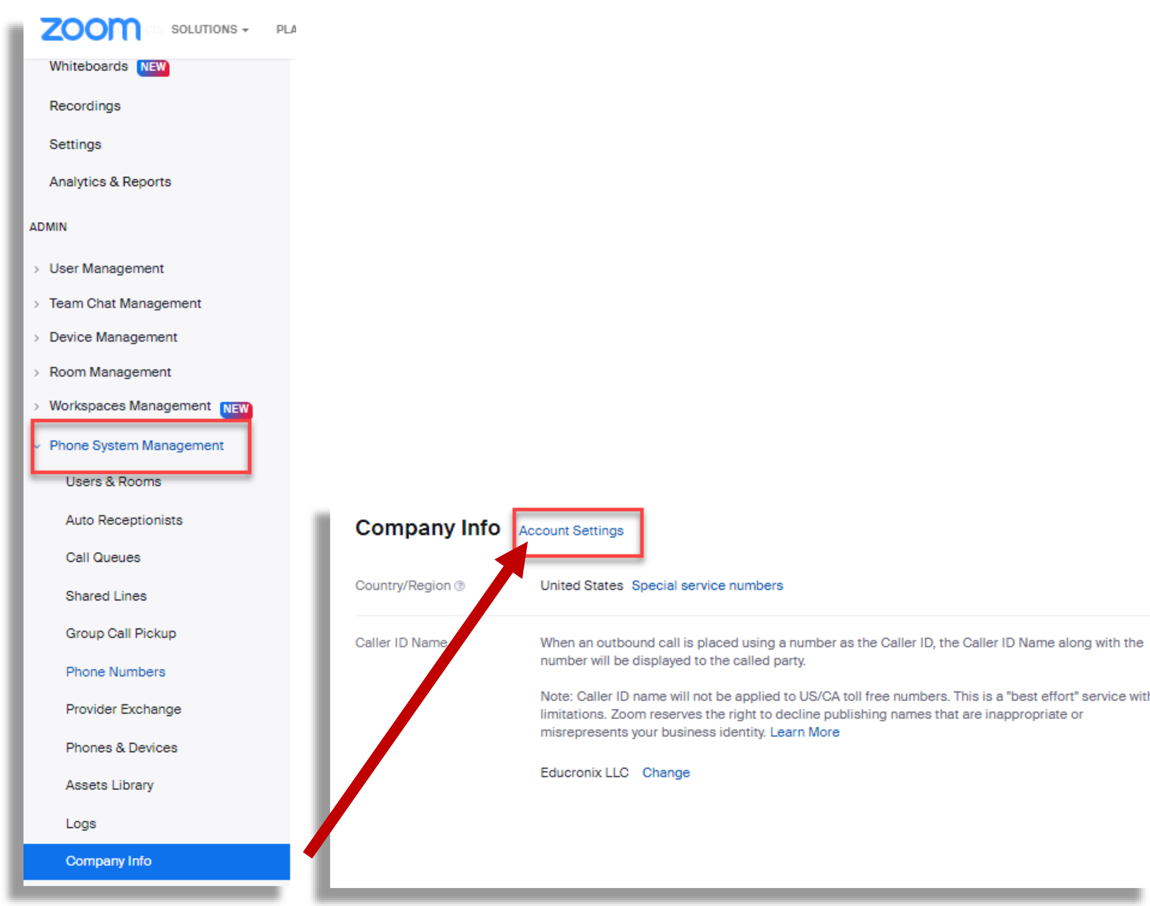
- SIParator® Reference Guide 6.4.1
- How to use Generic Header Manipulation
- Orientation and Installation – Ingate Software SIParator® Firewall/SIParator

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.

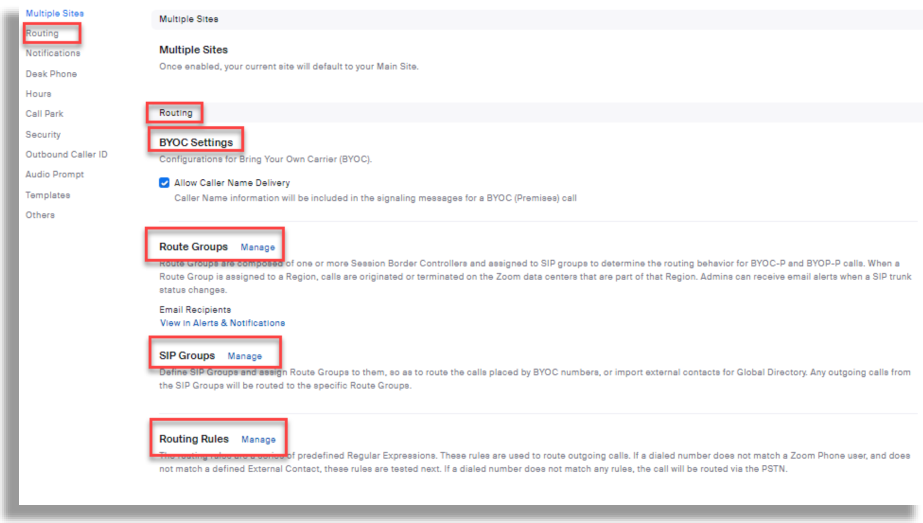
One you have it enable you'll notice the following fact in your Zoom Account dashboard.

First you'll notice a Phone System Admin section:



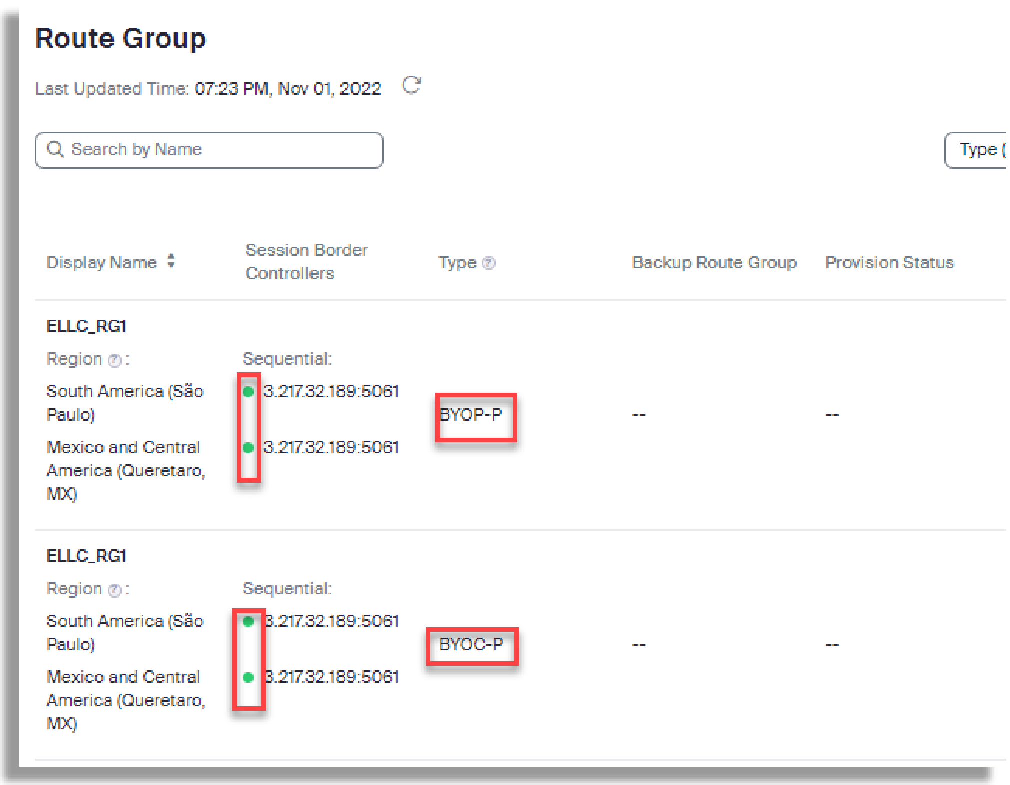
Select Company Info and then **Account Settings**

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



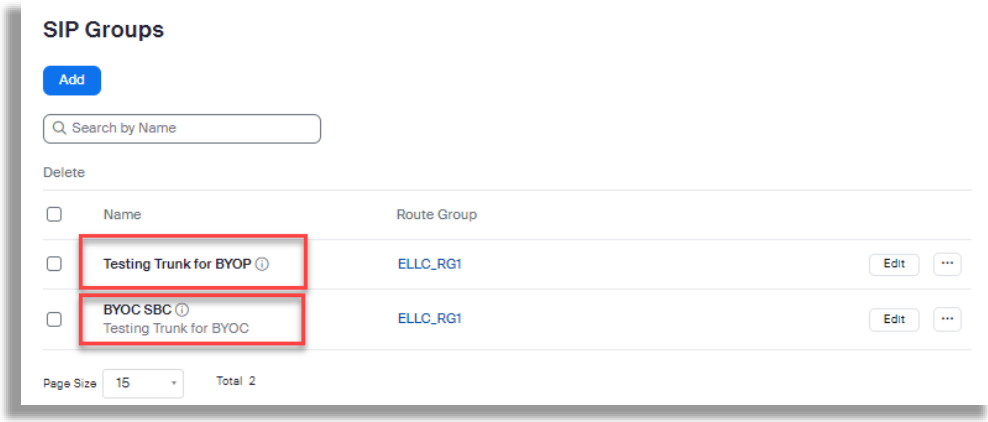
Route Groups (Manage)

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



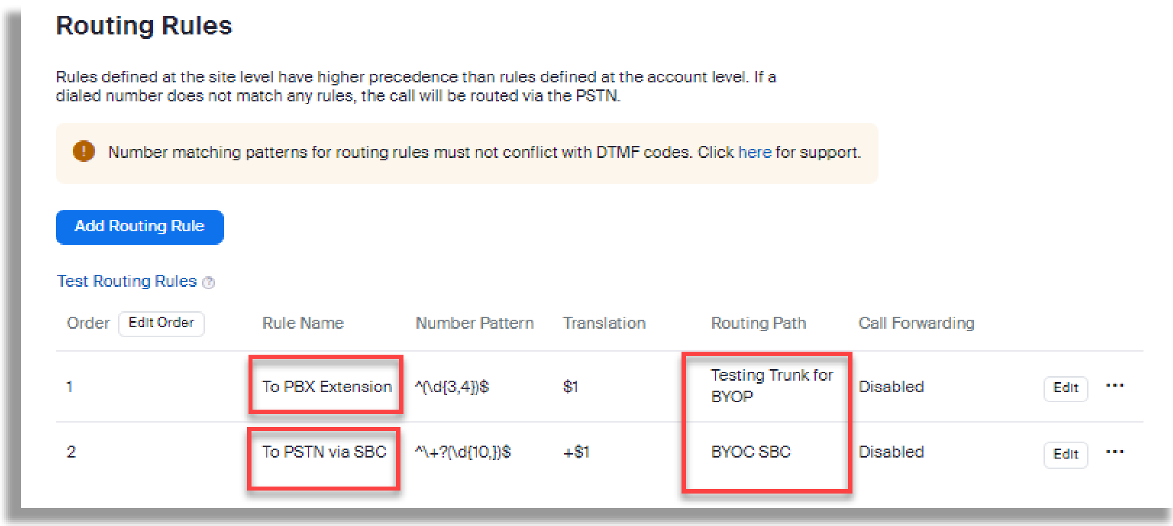
SIP Groups (Manage)

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



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).



Disclaimers

SIParator® and Ingate® are Trademarks of Ingate System AB

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

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