Ribbon EdgeMarc SBC Configuration with Zoom BYOC

Table of Contents

- Document Overview
- Non-Goals
- Audience
- Product and Device Details
- Network Topology Diagram
- Section A: EdgeMarc Configuration
    - Connectivity
    - Network
    - Static Routes
    - VoIP
    - SIP Settings
    - B2BUA
- Section B: Zoom Web BYOC Configuration
    - Add External Number
    - Create Zoom Users
    - Supplementary Services Configuration on Zoom
- Section C: TLS/SRTP Configuration between Ribbon EdgeMarc and Zoom

Document Overview

This document outlines the configuration best practices for the Ribbon EdgeMarc SBC when deployed with Zoom BYOC (Bring Your Own Carrier).

A Session Border Controller (SBC) is a network element deployed to protect SIP based Voice over Internet Protocol (VoIP) networks. Early deployments of SBCs were focused on the borders between two service provider networks in a peering environment. This role has now expanded to include significant deployments between a service provider's access network and a backbone network to provide service to residential and/or enterprise customers. The interoperability compliance testing focuses on verifying inbound and outbound calls flows between Ribbbon EdgeMarc and Zoom cloud. The Ribbon EdgeMarc SBC is deployed on the customer site to resolve any potential numbering format issues between Zoom and the customer's existing carrier dial plan numbering.

This guide contains the following sections:

- Section A: EdgeMarc Configuration
    - Captures general EdgeMarc configurations for deploying with Zoom BYOC.
- Section B: Zoom Web BYOC configuration
    - Captures the Zoom BYOC configuration.
    - All basic calls, along with the supplementary features like call hold, call transfer, and conference can be tested with configurations from Section A and Section B.
    - Advanced supplementary features can be configured on Zoom as mentioned in Supplementary Services Configuration on Zoom. These cover:
        - Auto Receptionist
        - Call Flip
        - Shared Line Appearance (SLA) or Call Delegation
        - Shared Line Group (SLG)
- Section C: TLS/SRTP Configuration Between Ribbon EdgeMarc and Zoom
    - Captures the TLS/SRTP configuration between EdgeMarc and Zoom cloud.
    - If transport is TLS and media is SRTP, follow the steps in this section, followed by B2BUA for routing, E.164 numbering, and header manipulations in Section A.

References
For additional information on Zoom, refer tohttps://zoom.us

For additional information on the Ribbon SBC, refer to https://ribboncommunications.com/

Non-Goals

It is not the goal of this guide to provide detailed configurations that will meet the requirements of every customer. Use this guide as a starting point and build the SBC configurations in consultation with network design and deployment engineers.

Audience

This is a technical document intended for telecommunications engineers with the purpose of configuring both the Ribbon SBCs and the third-party product. Steps will require navigating the third-party product as well as the Ribbon SBC Command Line Interface (CLI). Understanding the basic concepts of TCP/UDP, IP/Routing, and SIP/RTP is needed to complete the configuration and any necessary troubleshooting.

Note
This configuration guide is offered as a convenience to Ribbon customers. The specifications and information regarding the product in this guide are subject to change without notice. All statements, information, and recommendations in this guide are believed to be accurate but are presented without warranty of any kind, express or implied, and are provided “AS IS”. Users must take full responsibility for the application of the specifications and information in this guide.

Product and Device Details

The sample configuration in this document uses the following equipment and software:

Table 1: Requirements

	Equipment	Software Version
Ribbon Communications	Ribbon EdgeMarc 2900A	V15.8.0

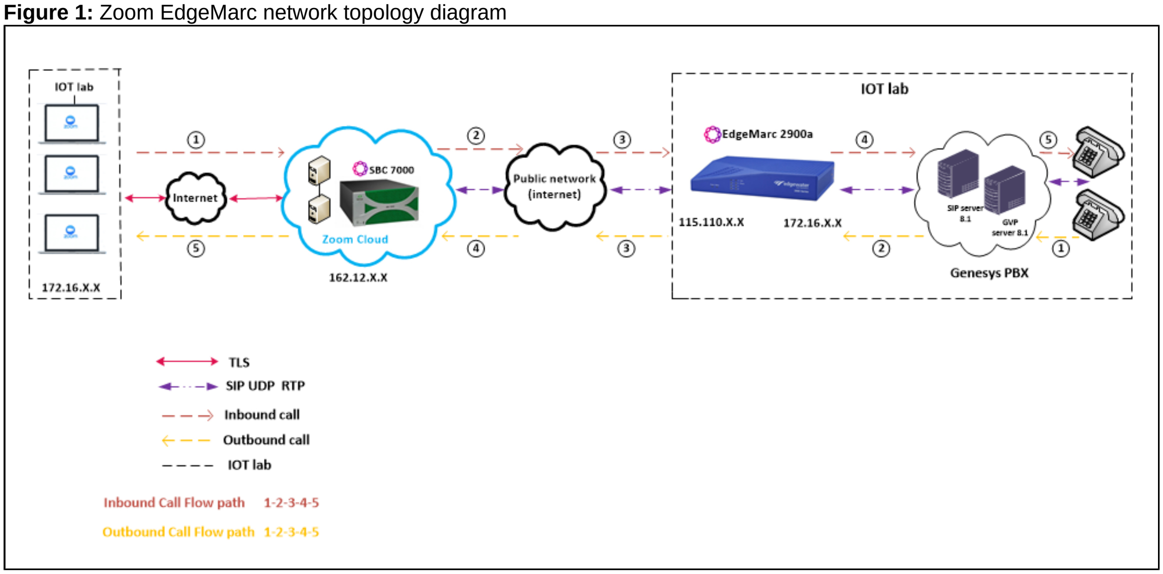
Zoom	Zoom app Desktop	4.6.10(20033.0407)
	Zoom app Mobile	4.6.11(20553.0413)
Third-party Equipment	Kapanga Softphone	1.00
	Phonerlite	2.77
	Zoiper	5.3.8

Configuration guide is designed keeping EdgeMarc 2900A as a representative model with the software version V15.8.0 but it applies to all models in the EdgeMarc portfolio (300, 2900, 480x, 6000, 7301, 7400) with same software version.

Network Topology Diagram

The following topology diagram shows connectivity between Zoom and Ribbon EdgeMarc 2900A.

Figure 1: Zoom EdgeMarc network topology diagram



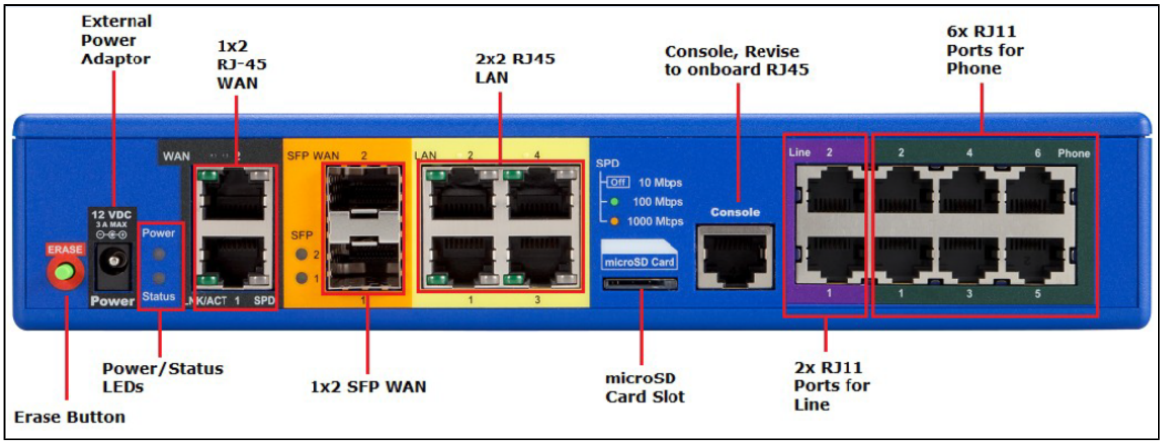
Section A: EdgeMarc Configuration

The following EdgeMarc configurations are included in this section:

1. Connectivity
2. Network
3. Static Routes
4. VoIP
5. B2BUA

Connectivity

Figure 2: EdgeMarc Back Panel



EdgeMarc 2900a interface/port details are listed in the table:

Figure 3: EgeMarc 2900a Interfaces

	EdgeMarc 2900a
Ports	
WAN 1Gb/s Ethernet (RJ-45)	2
Optical WAN 1 Gb/s ports (SFP)	2
LAN 1 Gb/s Ethernet (RJ-45)	4
FXO (RJ-11)	2
FXS (RJ-11)	6
Micro SD (SDXC) slot	1
Console (RJ-45)	1

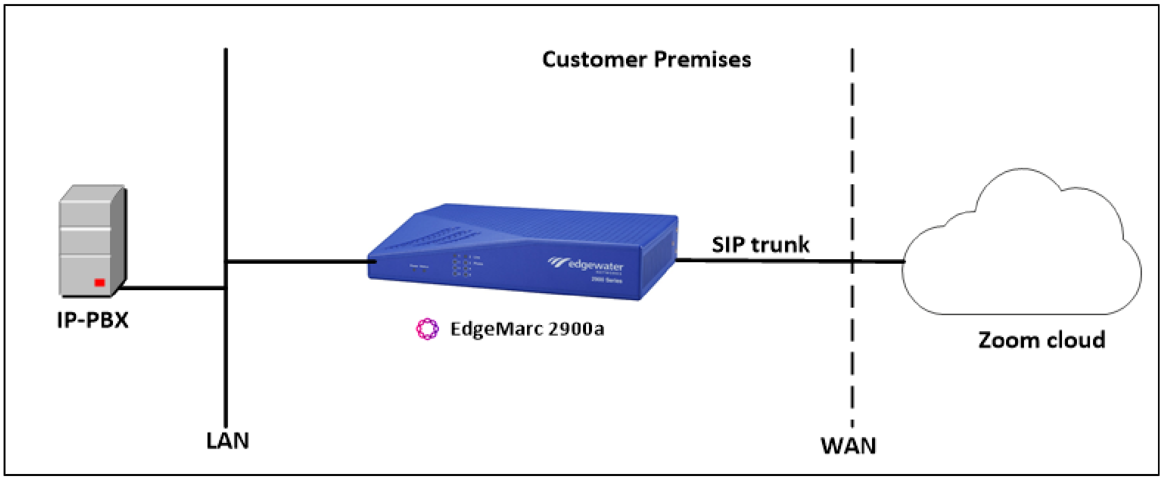
In the current test bed setup, the RJ45 port is used for both LAN and WAN interfaces

- **LAN Port** - RJ45 "LAN1" port is being used for LAN Side connectivity.
- **WAN Port** - RJ45 "WAN1" port is being used for WAN Side connectivity.

IP-PBX (PSTN side) is connected towards the LAN interface of EdgeMarc 2900a.

Zoom cloud is connected towards the WAN interface of EdgeMarc 2900a.

Figure 4: EdgeMarc Network Deployment



Network

Login to the EdgeMarc as root user and click *Network* to configure the LAN and WAN interfaces.

Figure 5: EdgeMarc Network LAN Interface

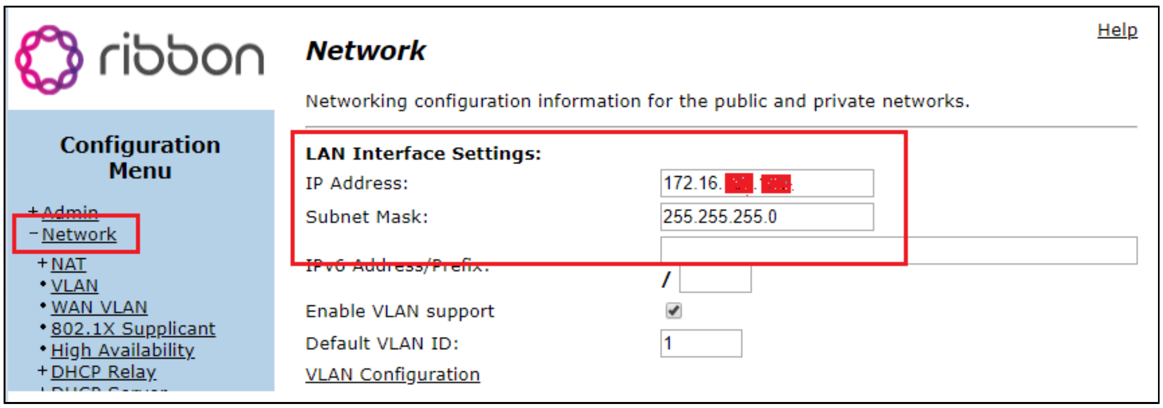
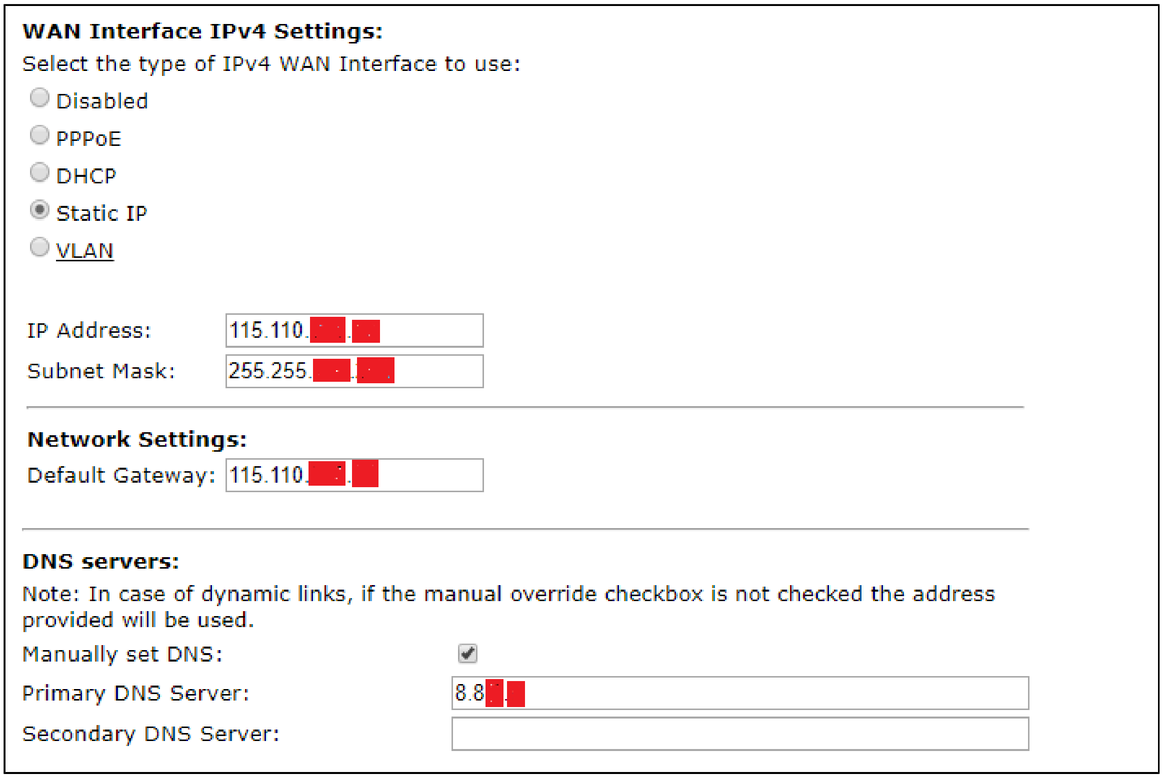


Figure 6: EdgeMarc Network WAN Interface and DNS configuration



Static Routes

Static routes are used to create communication to remote networks. In a production environment, static routes are mainly configured for routing from a specific network to a network that can only be accessed through one point or one interface (single path access or default route).

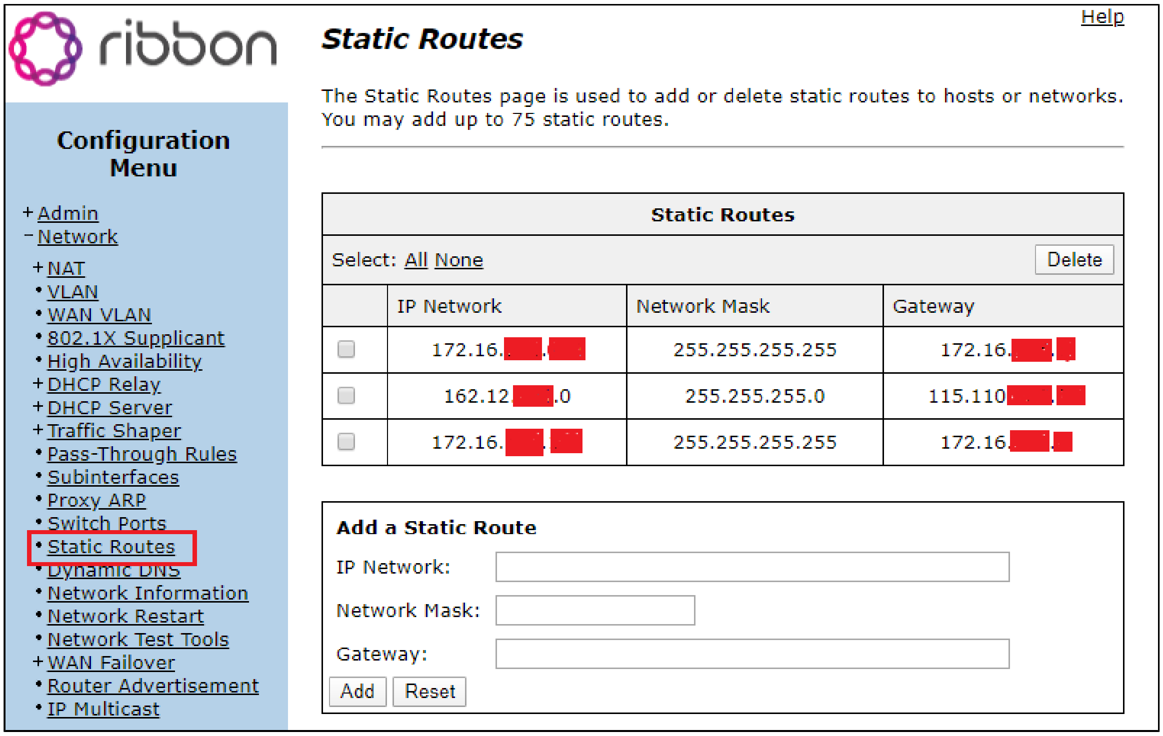
- For smaller networks with just one or two routes, configuring static routing is preferable. This is often more efficient since a link is not being wasted by exchanging dynamic routing information.
- For networks that have a LAN side Gateway on a Voice VLAN or Multi-Switch Edge Devices (MSEs) with voice VLAN towards EdgeMarc, static routing configurations are not required.

Static routes need to be added towards LAN interface 172.16.X.X(IP-PBX) and WAN interface 162.12.X.0(Zoom), as Zoom uses multiple IP's in this subnet.

172.16.X.X is the IP of the phone behind the IP-PBX. Add the static route for the media to also work.

- Navigate to **Network > Static Routes** to configure the routes.

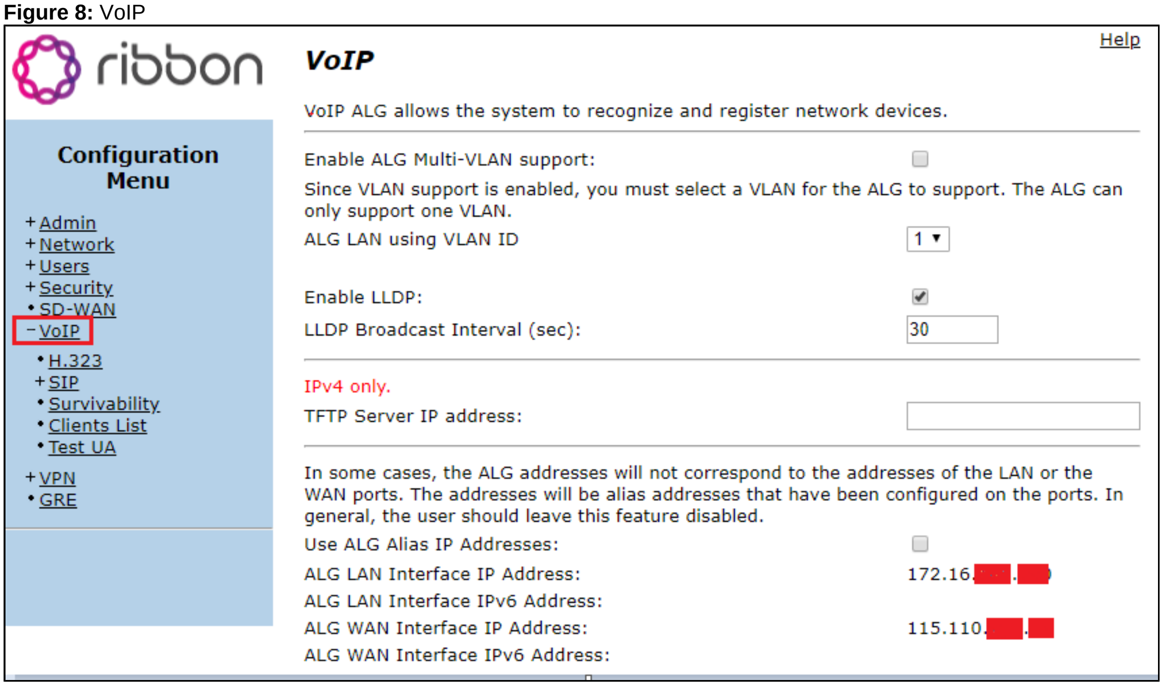
Figure 7: Static Routes



VoIP

Navigate to **VoIP** and check whether the LAN and WAN interfaces configured earlier are reflected accordingly.

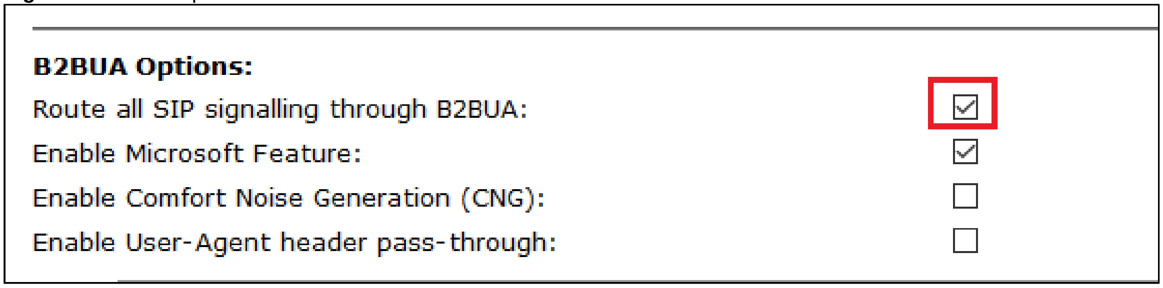
Figure 8: VoIP



Check the following option *"Route all SIP signalling through B2BUA"*

PSTN side is not expected to send Comfort Noise packets on Mute. However, it might send out empty RTP packets towards EdgeMarc. It is recommended to uncheck the following option "*Enable Comfort Noise Generation(CNG)*" so that EdgeMarc does not generate Comfort Noise packets towards Zoom.

Figure 9: B2BUA Options



SIP Settings

1. Navigate to **VoIP > SIP** to configure the SIP settings.
2. Configure the SIP server address as the Zoom SIP server IP (for example, 162.12.X.X in our case).
3. Keep the B2BUA, UDP, and TCP settings at the default configuration.

Figure 10: SIP

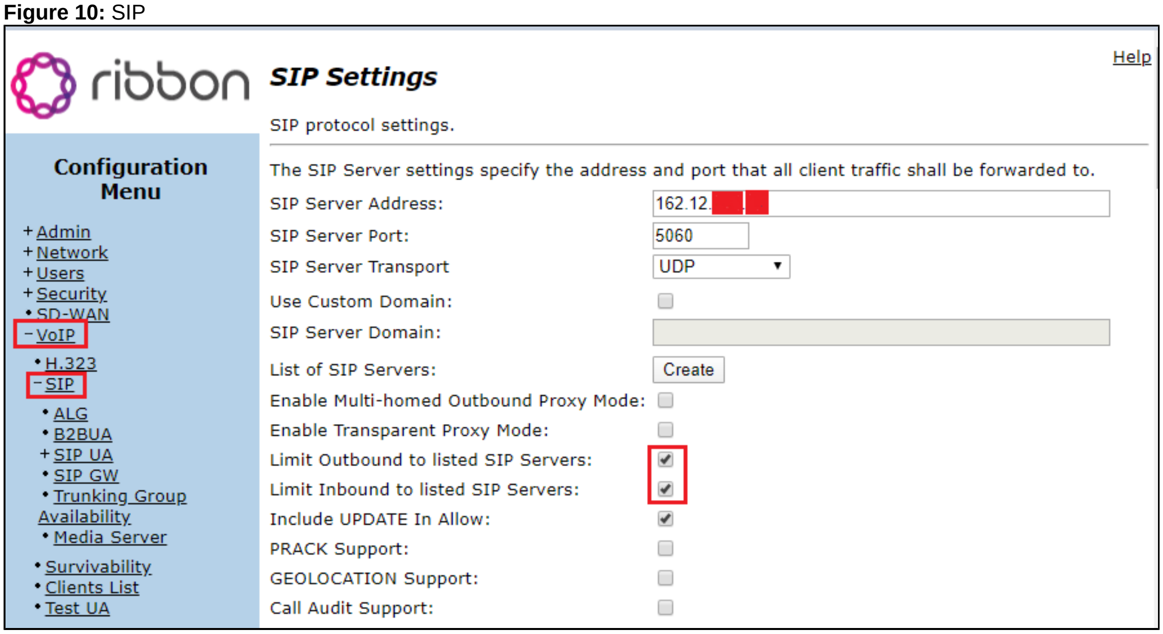


Figure 11: B2BUA Options

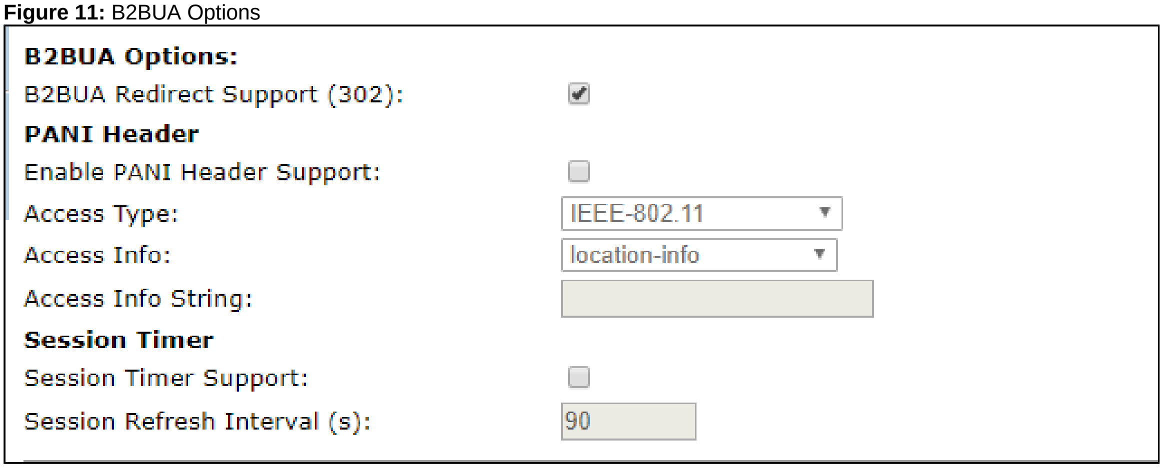


Figure 12: UDP TCP default settings

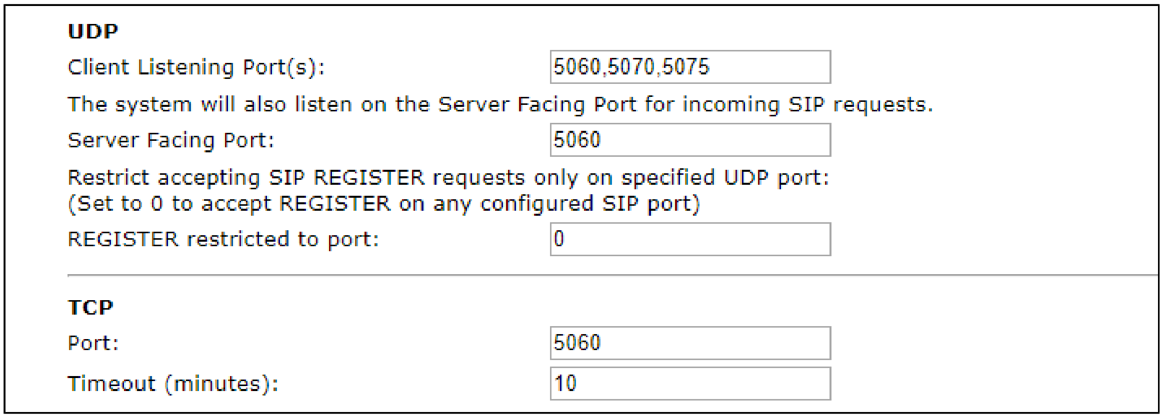
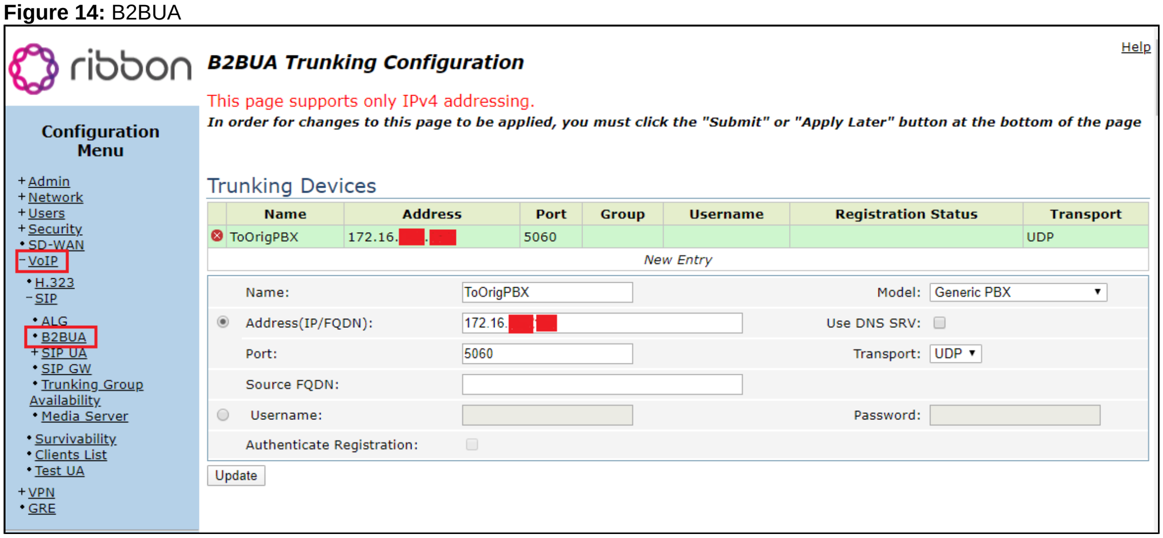


Figure 13: SDP - default settings

B2BUA

1. Navigate to **VoIP > SIP > B2BUA**
2. Configure the IP address of the IP-PBX (for example, 172.16X.X in our case).

Figure 14: B2BUA



E.164 Country code Mapping

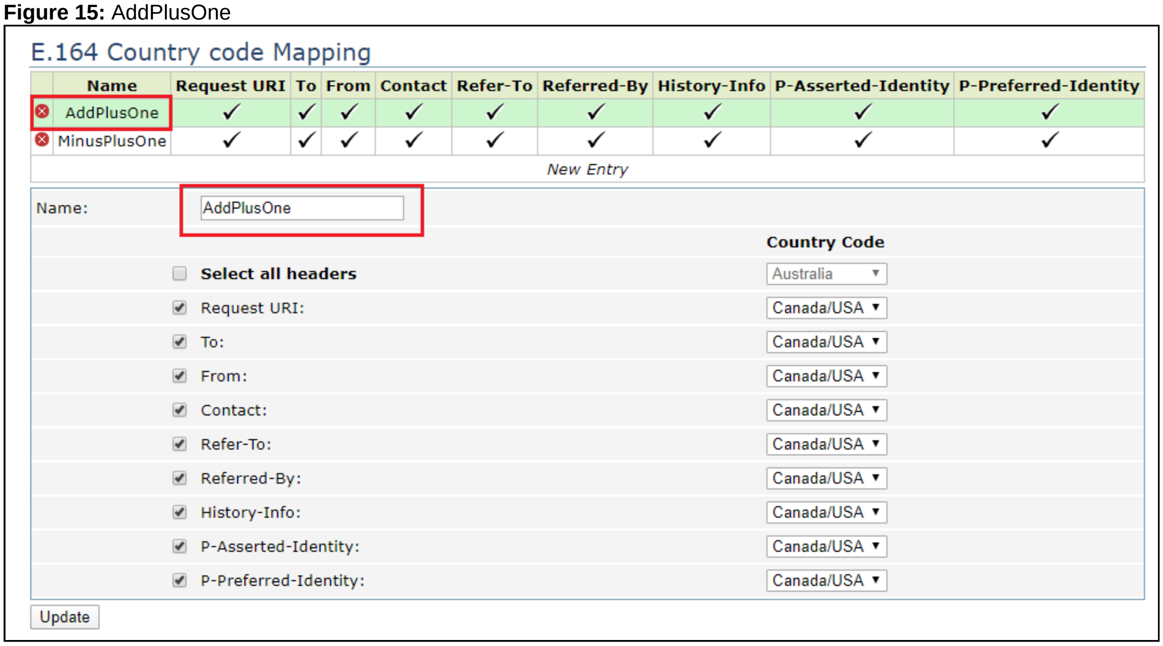
Example: A customer has an existing carrier that only accepts U.S.A. domestic 10 digit dial plan numbering format. For example: (XXX) YYY-ZZZZ, where XXX=area code, YYY-ZZZZ=7-digit phone number. At the same time, Zoom is using the E.164 numbering format: +(country code)(phone number). This has created a phone number format incompatibility issue between Zoom and the customer carrier. Zoom expects to receive calls in E.164 numbering format, while the customer carrier expects the USA 10-digit domestic numbering format. EdgeMarc SBC is introduced to solve the numbering interop issue between the two entities. The EdgeMarc SBC inserts a “+1” for all U.S. phone numbers destined for Zoom, and removes “+1” for all U.S. phone numbers destined for customer carrier(s).

> **Note**
> Ribbon EdgeMarc SBC can be programmed for different country E.164 code mapping in addition to the U.S. dial plan.

The following rule is required to "Add +1" to outgoing call towards Zoom.

1. Name the Rule as "AddPlusOne".
2. Check all headers and set the Country Code to "Canada/USA".

Figure 15: AddPlusOne



The following rule is required to "Remove +1" to call towards IP-PBX.

1. Name the Rule as "MinusPlusOne".
2. Check all headers and set the Country Code to "Canada/USA".

Figure 16: MinusPlusOne

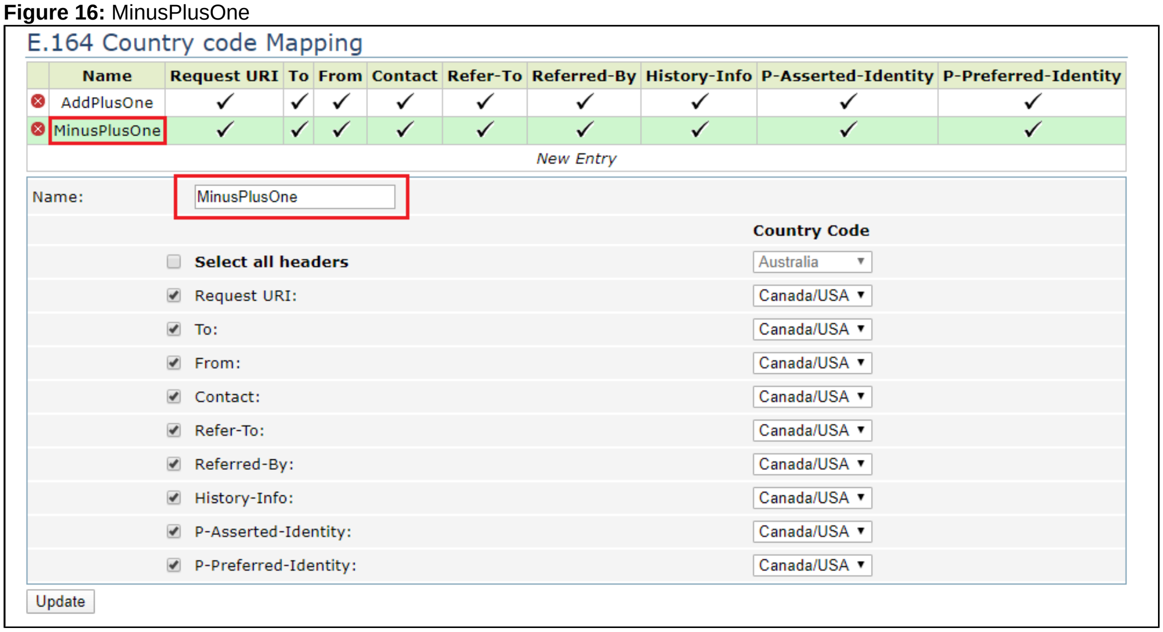


Figure 17: Actions - ToZoomCloud

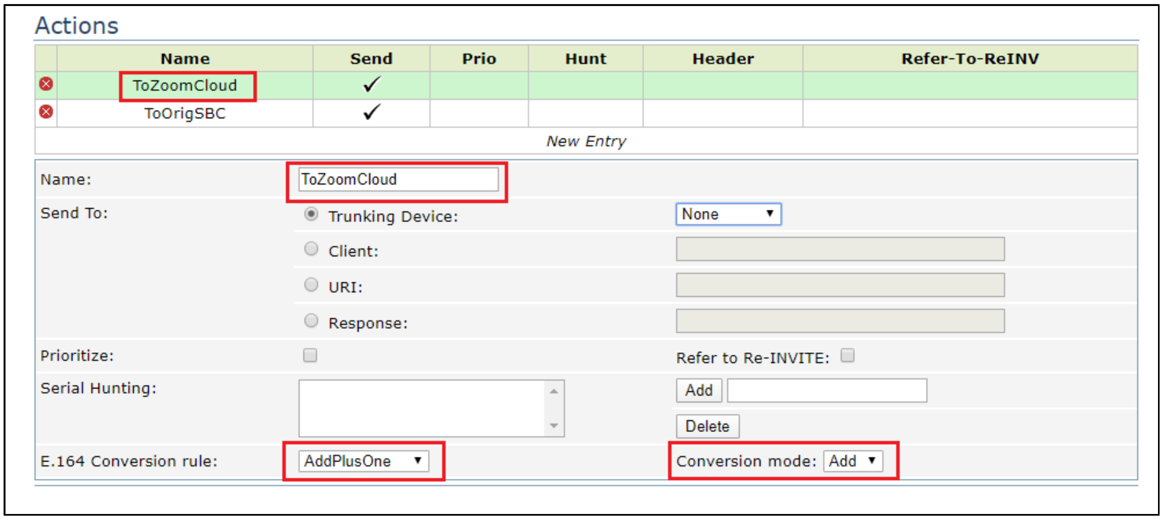


Figure 18: Actions - ToOrigPBX

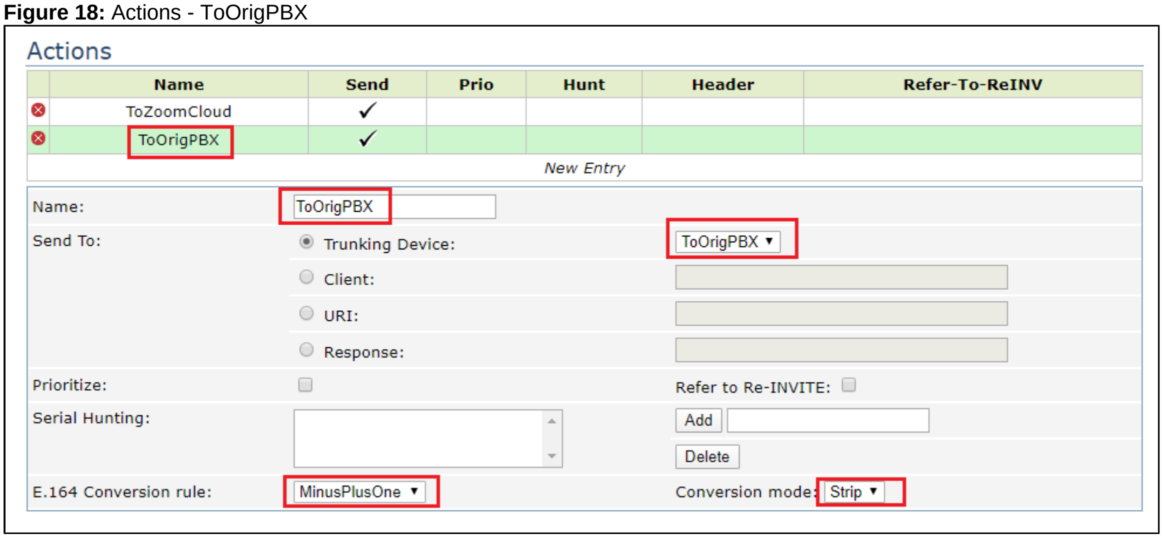


Figure 19: Match - Outbound

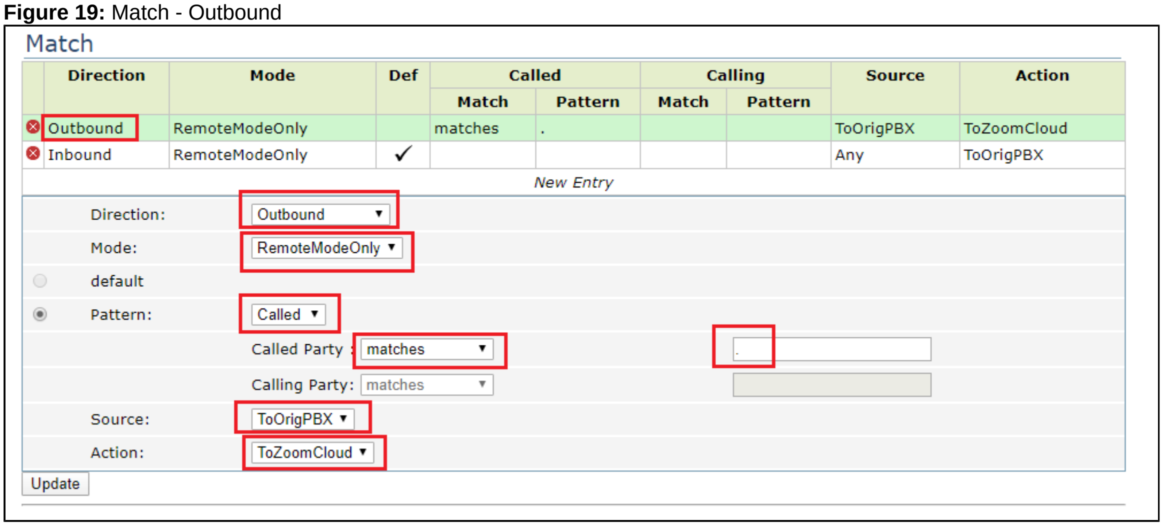
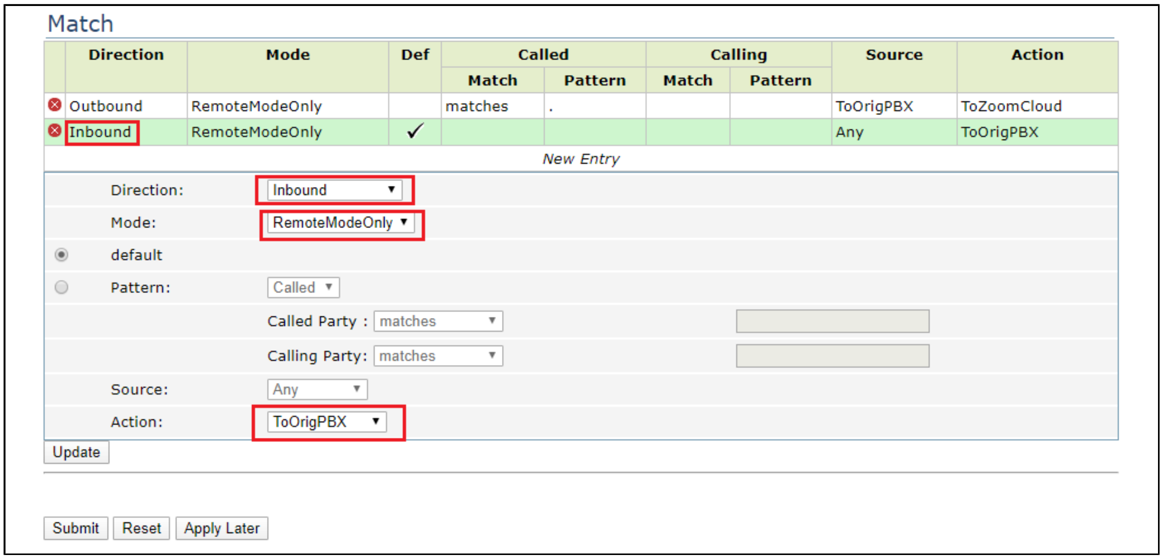


Figure 20: Match - Inbound



Section B: Zoom Web BYOC Configuration

Prerequisites:

- Zoom Go BYOC account: A special type of Zoom account that has outbound/inbound SIP trunk that peers between the Zoom Phone Cloud and the customer's PSTN carrier connection.
- Customer's existing carrier/carrier equipment: any carrier offering PSTN services. Carrier equipment can be router/gateway or another SBC that supports SIP trunk connectivity. IP-PBX was used to simulate customer carrier router/gw. Carrier has provided several DID's to use as external BYOC numbers.
- Trunk Registration: BYOC is a "static" trunk between 2 static IP endpoints, therefore no trunk registration is done here.

> **Note**
> Ensure a Zoom BYOC SIP trunk is built between Zoom SBC and EdgeMarc SBC deployed on a customer site.

Once the Zoom Go account is available, login to Zoom Web BYOC portal at https://go.zoom.us/.

The following Zoom BYOC configurations are included in this section:

1. Add External Number.
2. Create Zoom Users.
3. Supplementary services configuration on Zoom.

Add External Number

Navigate to **Phone Systems Management > Phone Numbers > External**

Select **Add** to add external phone numbers provided by your carrier into Zoom portal. These numbers are the DID numbers provided by your carrier.

Figure 21: Add External Number

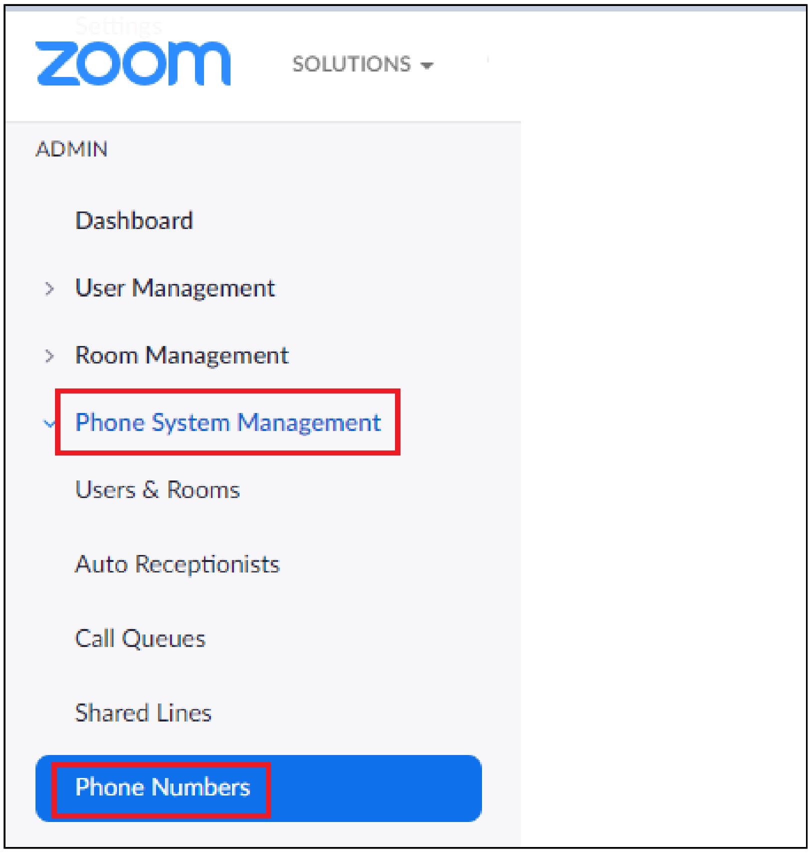
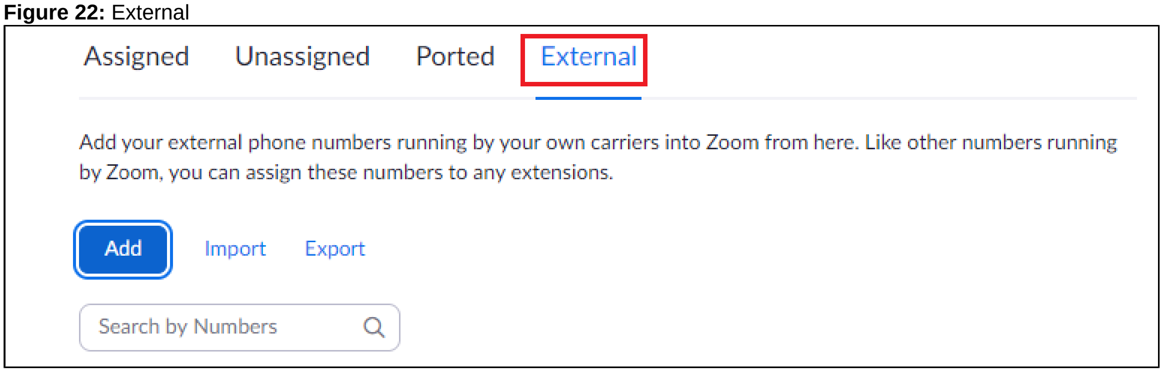
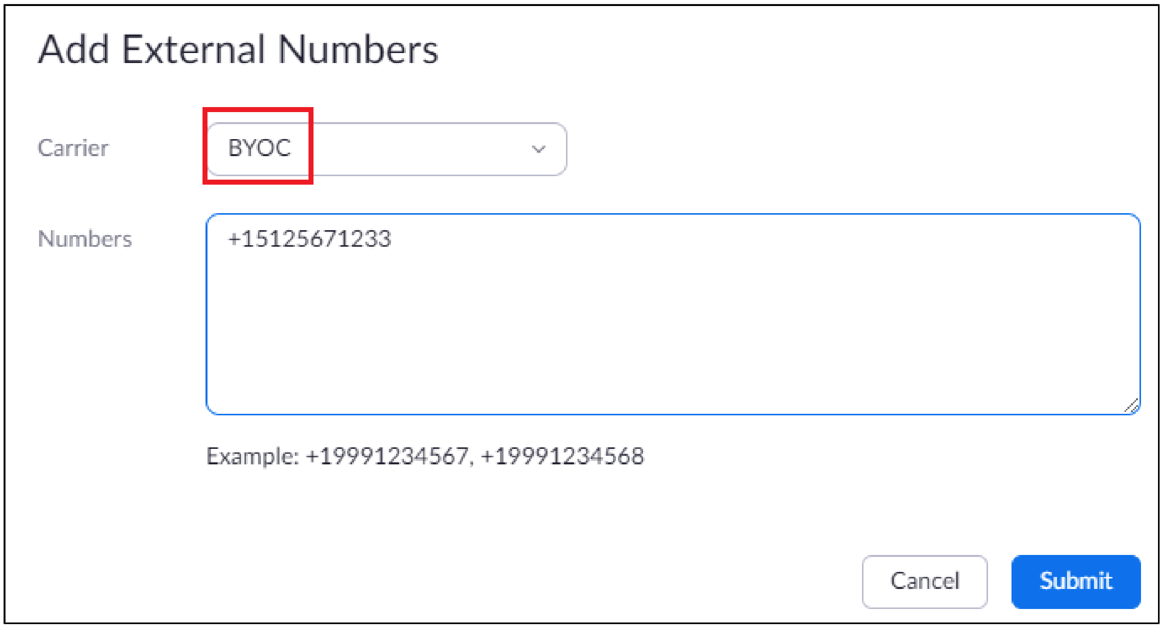


Figure 22: External



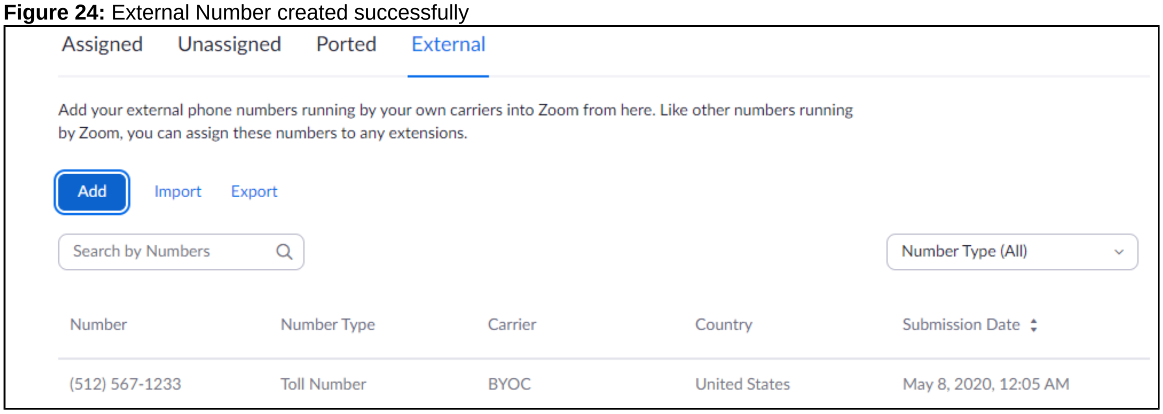
Select **BYOC** as the carrier and enter the customer existing phone numbers (from carrier) separated by commas. Click **Submit**.

Figure 23: Add External Number



Verify the external numbers have been created successfully as shown below.

Figure 24: External Number created successfully



Create Zoom Users

Zoom Users are created in order to login to Zoom clients on a desktop or mobile. Create a user as follows:

1. Navigate to **User Management > Users**. *Click* **Add** to create new Zoom users.
2. Navigate to **Phone System Management > Users & Rooms.** *Check for the User status "***Active***".*
3. Navigate to **Assign Calling Plan > Assign BYOC Calling Plan***.* Click on *"***Confirm and Assign Numbers***".*

Figure 25: Create Zoom User

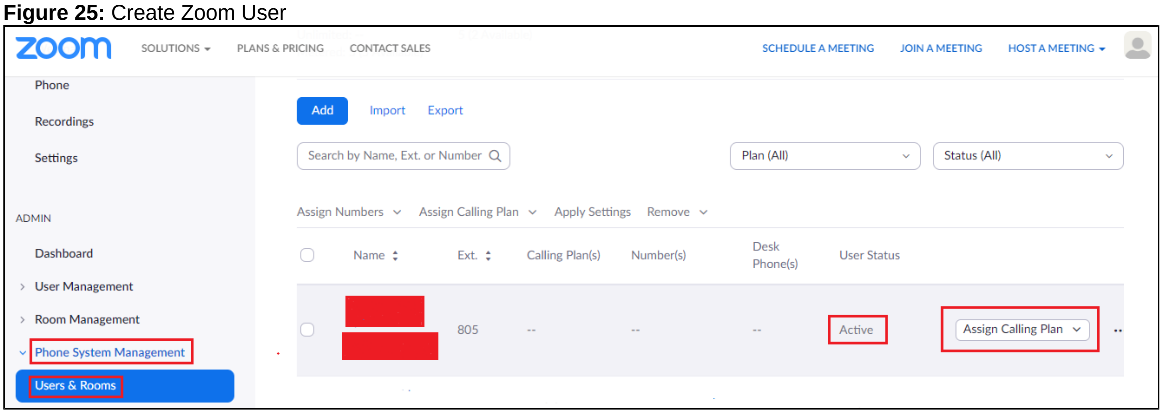
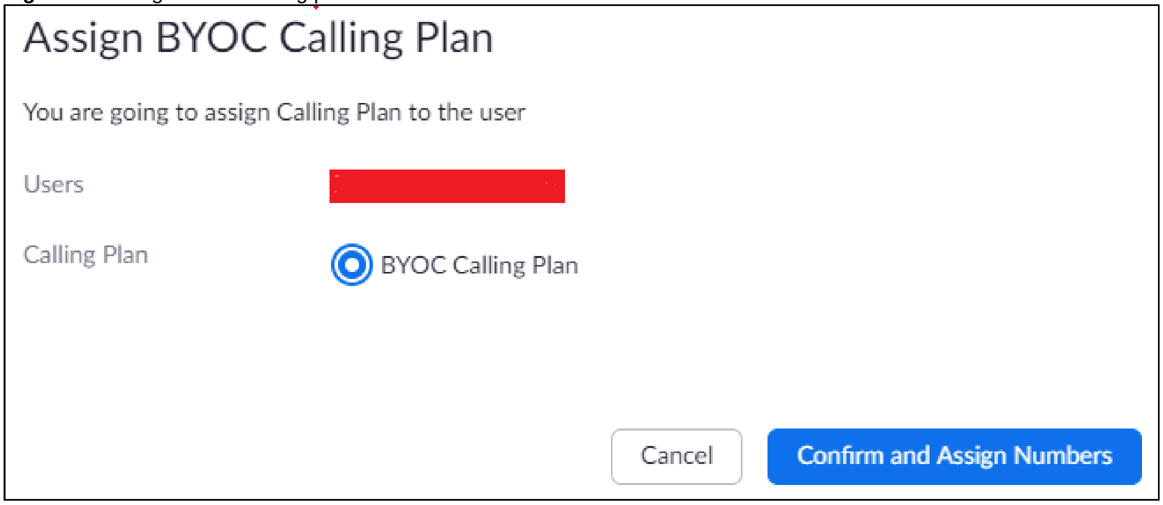
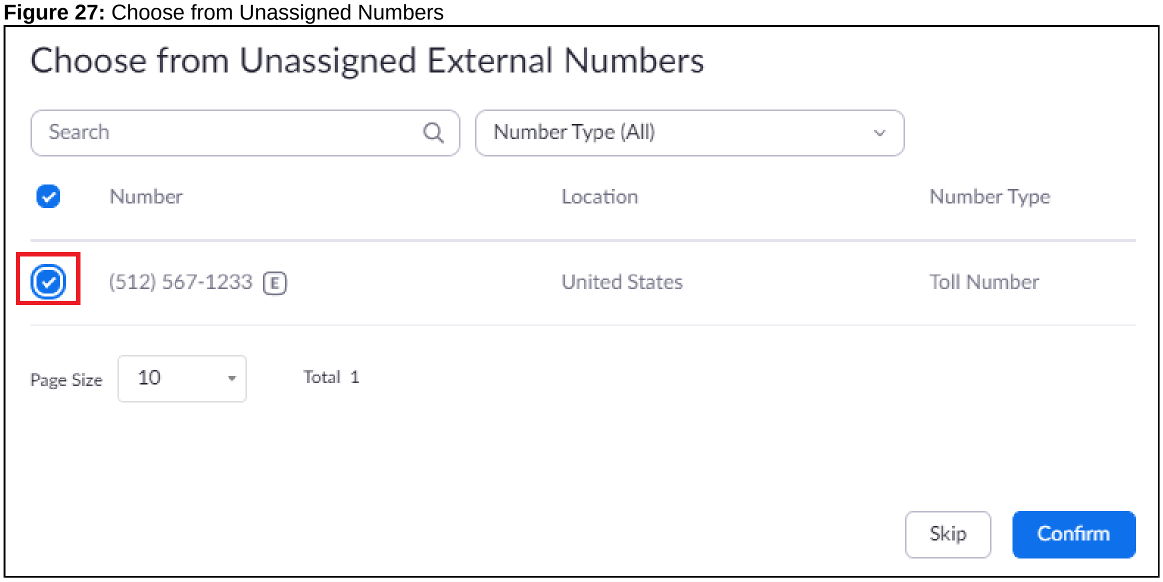


Figure 26: Assign BYOC calling plan



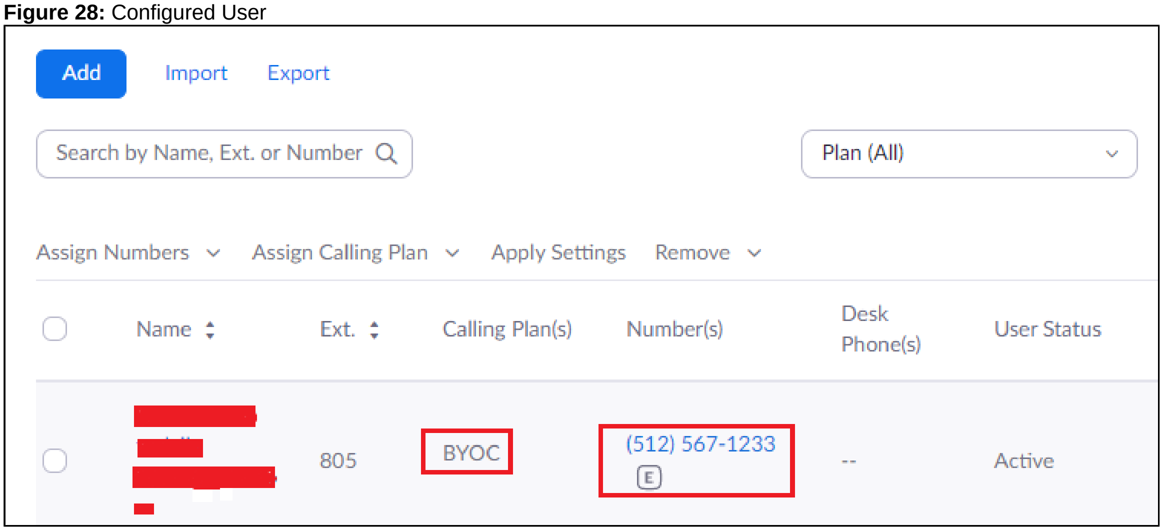
4. Assign the External Numbers created previously in the Add External Number section.

Figure 27: Choose from Unassigned Numbers



5. Click **Confirm** to finish. Once the User is assigned with a Calling Plan and Number, it should look like the following example.

Figure 28: Configured User



Supplementary Services Configuration on Zoom

Zoom supports multiple supplementary services. To configure different supplementary services in Zoom, refer to the following links:

1. Auto Receptionist: https://support.zoom.us/hc/en-us/articles/360001297663-Getting-started-with-Zoom-Phone-admin-#h_a625f531-94c6-4291-909e-3d68ad685b68

2. Call Flip: https://support.zoom.us/hc/en-us/articles/360034613311-Using-Call-Flip

3. Shared Line Appearance (SLA) or Call Delegation: https://support.zoom.us/hc/en-us/articles/360032881731

4. Shared Line Group/SLG: https://support.zoom.us/hc/en-us/articles/360038850792/

Section C: TLS/SRTP Configuration between Ribbon EdgeMarc and Zoom

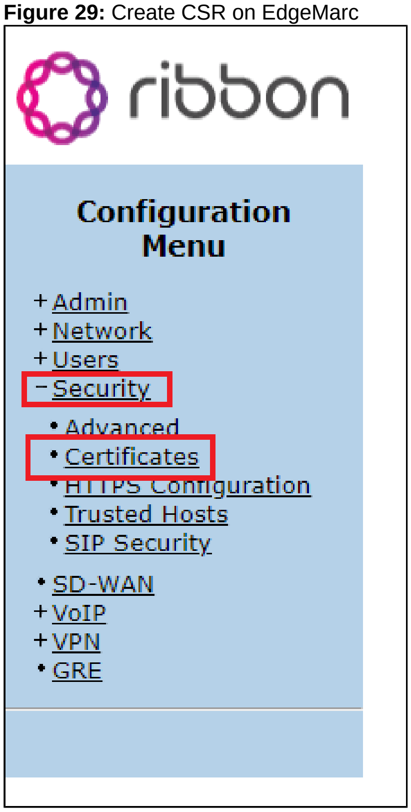
Prerequisites:

- As the TLS needs to performed on the WAN side, a trusted CA (Certificate Authority) is needed. In this scenario, GoDaddy is used as a Trusted CA.
- Zoom BYOC trunk should be enabled with TLS/SRTP.

Generate a CSR from EdgeMarc SBC

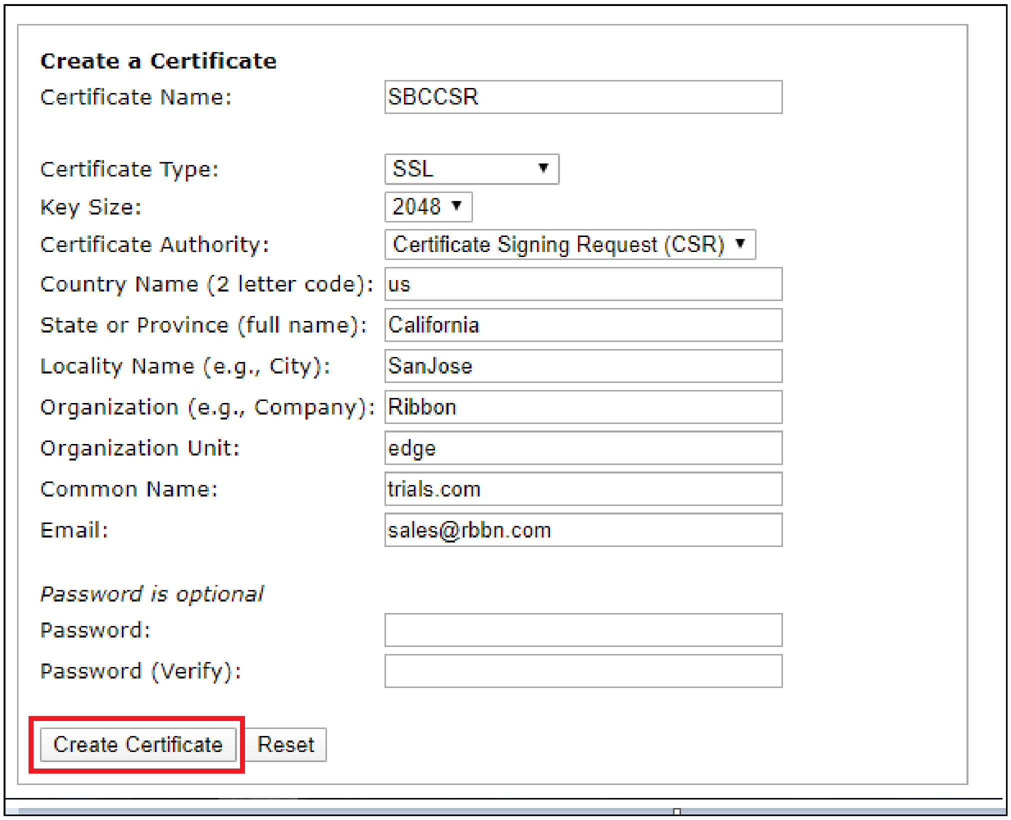
1. Navigate to **Security > Certificates**.

Figure 29: Create CSR on EdgeMarc



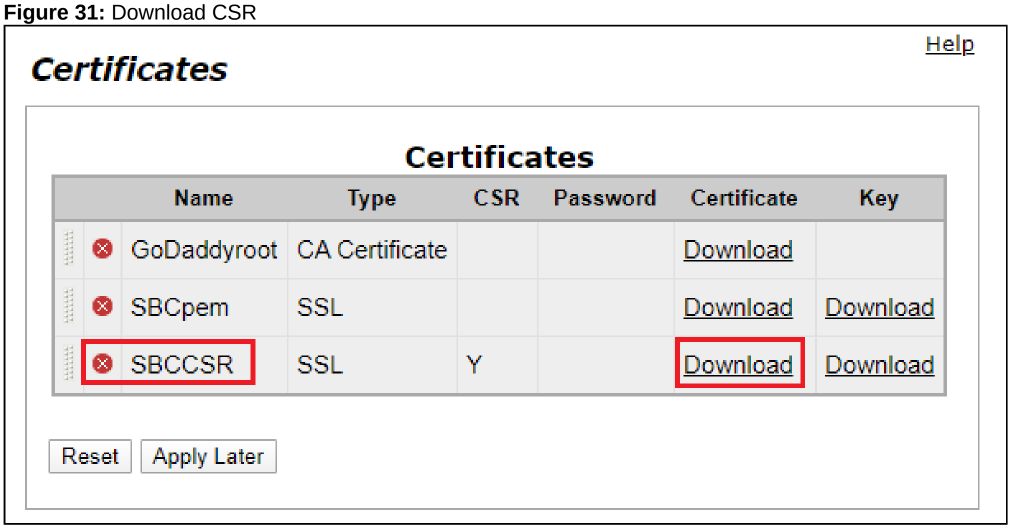
2. Fill in the details as specified below:
   a. Common name: should be the valid fqdn, here "trials.com" is given as a sample configuration.
   b. Email: Provide the valid Email ID.

Figure 30: Certificates



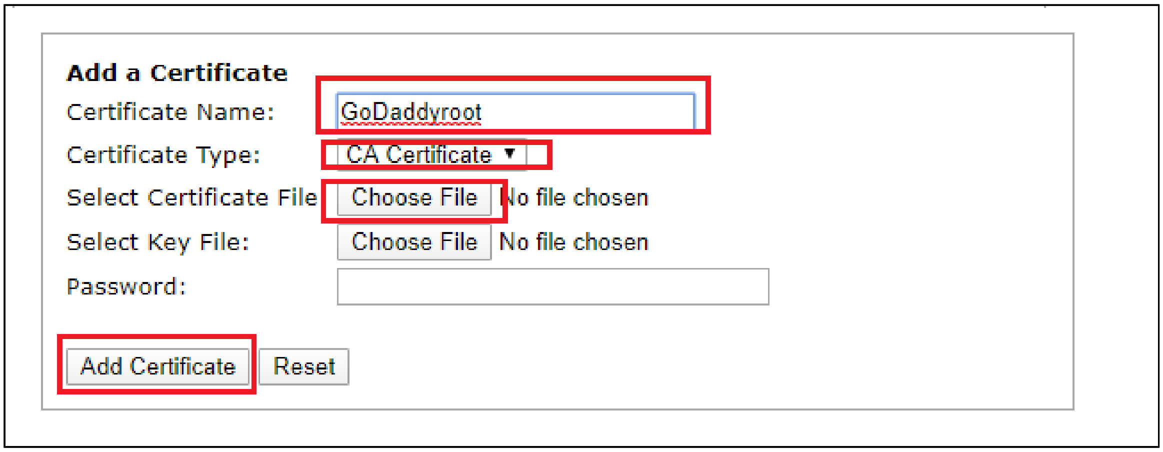
3. Download the CSR certificate from SBC and get it signed from a Trusted CA.

Figure 31: Download CSR



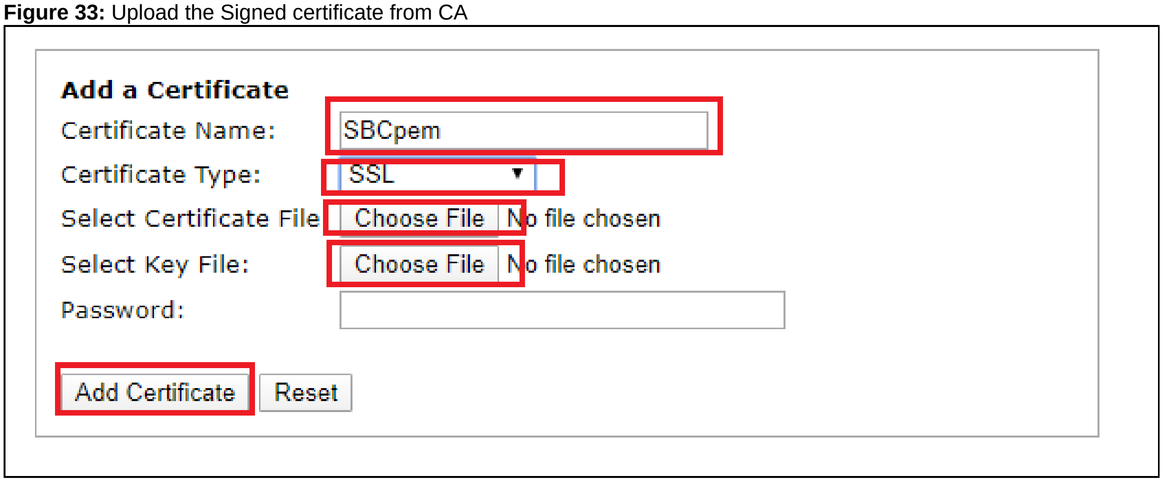
4. Obtain the Root certificate and EdgeMarc SBC signed certificate from the Trusted CA and upload as follows: Key file and Password is not required.

Figure 32: Upload Root certificate



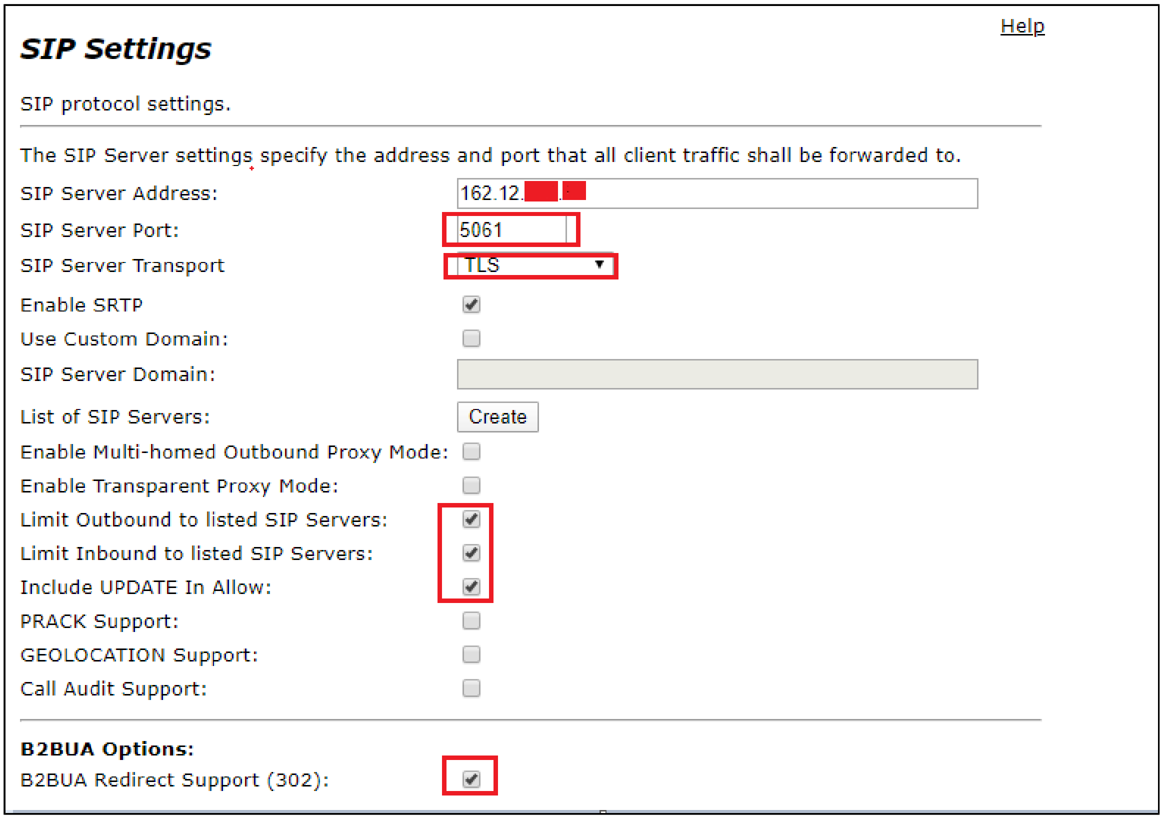
5. Upload the Signed certificate from CA as follows:
    a. Certificate Name: SBCpem (in our case).
    b. Certificate Type: SSL.
    c. Select certificate file: Signed SBC certificate from Trusted CA.
    d. Select Key file: Private key of SBC.

Figure 33: Upload the Signed certificate from CA



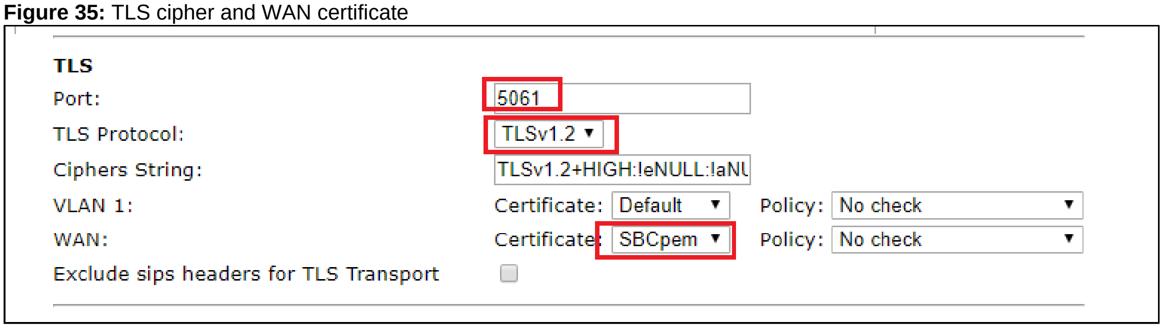
6. Navigate to **VoIP > SIP.**
    a. Apply the following settings as mentioned below.

Figure 34: SIP Settings



7. Choose the SBCpem certificate that was uploaded in a previous step.

Figure 35: TLS cipher and WAN certificate



8. SRTP calls need the following configuration:
   a. Navigate to **VoIP > Media Security**.

Figure 36: SRTP config