

---

# 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 Ribbon 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 to <https://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
<b>Ribbon Communications</b>	Ribbon EdgeMarc 2900A	V15.8.0

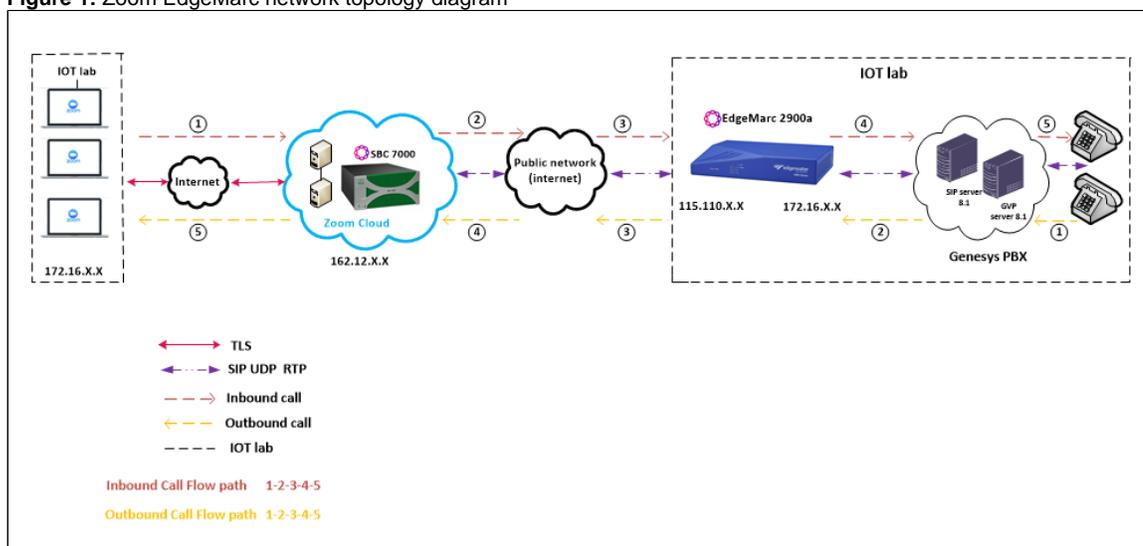
<b>Zoom</b>	Zoom app Desktop	4.6.10(20033.0407)
	Zoom app Mobile	4.6.11(20553.0413)
<b>Third-party Equipment</b>	Kapanga Softphone	1.00
	Phonerlite	2.77
	Zoiper	5.3.8

 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



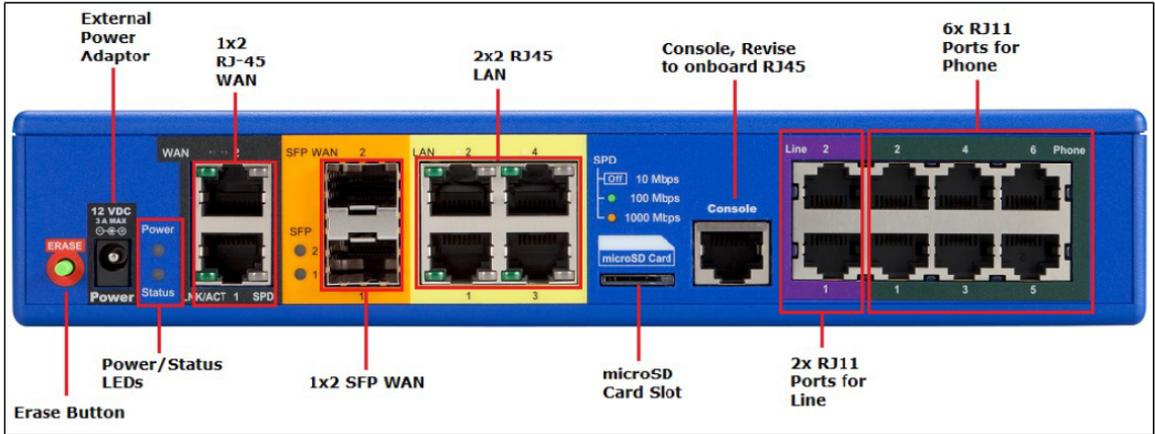
## Section A: EdgeMarc Configuration

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:** EdgeMarc 2900a Interfaces

EdgeMarc 2900a	
<b>Ports</b>	
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



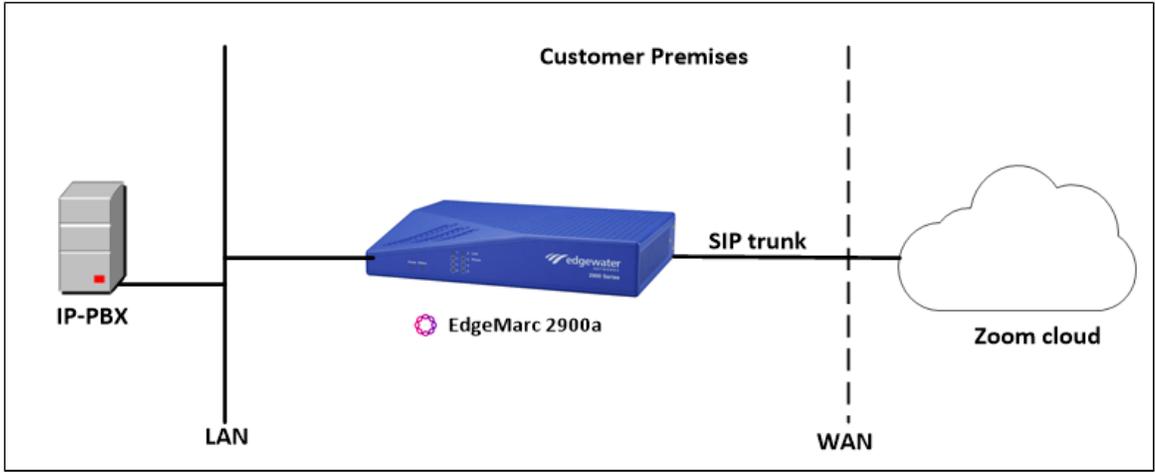
In the current test bed setup, the RJ45 port is used for both LAN and WAN interfaces

- **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

The screenshot shows the EdgeMarc Network configuration interface. The 'LAN Interface Settings' section is highlighted with a red box, showing the following configuration:

- IP Address: 172.16.1.1
- Subnet Mask: 255.255.255.0
- IPv6 Address/Prefix: /
- Enable VLAN support:
- Default VLAN ID: 1

The 'Configuration Menu' on the left shows the following options:

- + Admin
- Network
- + NAT
- VLAN
- WAN VLAN
- 802.1X Supplicant
- High Availability
- + DHCP Relay
- + DHCP Server

Figure 6: EdgeMarc Network WAN Interface and DNS configuration

### WAN Interface IPv4 Settings:

Select the type of IPv4 WAN Interface to use:

- Disabled
- PPPoE
- DHCP
- Static IP
- VLAN

IP Address:

Subnet Mask:

### Network Settings:

Default Gateway:

### DNS servers:

Note: In case of dynamic links, if the manual override checkbox is not checked the address provided will be used.

Manually set DNS:

Primary DNS Server:

Secondary DNS Server:

## 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



## Static Routes

The Static Routes page is used to add or delete static routes to hosts or networks. You may add up to 75 static routes.

Select: [All](#) [None](#) Delete

	IP Network	Network Mask	Gateway
<input type="checkbox"/>	172.16. [redacted]. [redacted]	255.255.255.255	172.16. [redacted]. [redacted]
<input type="checkbox"/>	162.12 [redacted].0	255.255.255.0	115.110 [redacted]. [redacted]
<input type="checkbox"/>	172.16. [redacted]. [redacted]	255.255.255.255	172.16. [redacted]. [redacted]

### Add a Static Route

IP Network:

Network Mask:

Gateway:

### Configuration Menu

- + Admin
- Network
- + NAT
- VLAN
- WAN VLAN
- 802.1X Supplicant
- High Availability
- + DHCP Relay
- + DHCP Server
- + Traffic Shaper
- Pass-Through Rules
- Subinterfaces
- Proxy ARP
- Switch Ports
- **Static Routes**
- Dynamic DNS
- Network Information
- Network Restart
- Network Test Tools
- + WAN Failover
- Router Advertisement
- IP Multicast

## VoIP

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

Figure 8: VoIP



## VoIP

VoIP ALG allows the system to recognize and register network devices.

Enable ALG Multi-VLAN support:

Since VLAN support is enabled, you must select a VLAN for the ALG to support. The ALG can only support one VLAN.

ALG LAN using VLAN ID:

Enable LLDP:

LLDP Broadcast Interval (sec):

**IPv4 only.**

TFTP Server IP address:

In some cases, the ALG addresses will not correspond to the addresses of the LAN or the WAN ports. The addresses will be alias addresses that have been configured on the ports. In general, the user should leave this feature disabled.

Use ALG Alias IP Addresses:

ALG LAN Interface IP Address: 172.16. [redacted]. [redacted]

ALG LAN Interface IPv6 Address:

ALG WAN Interface IP Address: 115.110 [redacted]. [redacted]

ALG WAN Interface IPv6 Address:

### Configuration Menu

- + Admin
- + Network
- + Users
- + Security
- SD-WAN
- **VoIP**
- H.323
- + SIP
- Survivability
- Clients List
- Test UA
- + VPN
- GRE



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

<b>B2BUA Options:</b>	
Route all SIP signalling through B2BUA:	<input checked="" type="checkbox"/>
Enable Microsoft Feature:	<input checked="" type="checkbox"/>
Enable Comfort Noise Generation (CNG):	<input type="checkbox"/>
Enable User-Agent header pass-through:	<input type="checkbox"/>

## 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

**ribbons SIP Settings** [Help](#)

SIP protocol settings.

The SIP Server settings specify the address and port that all client traffic shall be forwarded to.

SIP Server Address: 162.12.X.X

SIP Server Port: 5060

SIP Server Transport: UDP

Use Custom Domain:

SIP Server Domain: [Empty]

List of SIP Servers: [Create](#)

Enable Multi-homed Outbound Proxy Mode:

Enable Transparent Proxy Mode:

Limit Outbound to listed SIP Servers:

Limit Inbound to listed SIP Servers:

Include UPDATE In Allow:

PRACK Support:

GEOLOCATION Support:

Call Audit Support:

Figure 11: B2BUA Options

<b>B2BUA Options:</b>	
B2BUA Redirect Support (302):	<input checked="" type="checkbox"/>
<b>PANI Header</b>	
Enable PANI Header Support:	<input type="checkbox"/>
Access Type:	IEEE-802.11
Access Info:	location-info
Access Info String:	[Empty]
<b>Session Timer</b>	
Session Timer Support:	<input type="checkbox"/>
Session Refresh Interval (s):	90

Figure 12: UDP TCP default settings

**UDP**

Client Listening Port(s):

The system will also listen on the Server Facing Port for incoming SIP requests.

Server Facing Port:

Restrict accepting SIP REGISTER requests only on specified UDP port:  
(Set to 0 to accept REGISTER on any configured SIP port)

REGISTER restricted to port:

---

**TCP**

Port:

Timeout (minutes):

Figure 13: SDP - default settings

**SDP Modifications**

SDP Codec Operation:

SDP Section that will be modified:

Codecs (comma separated list):

Reject when No Match Codec:

Strip Matched Expressions:

**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

**Configuration Menu**

- + Admin
- + Network
- + Users
- + Security
- + SD-WAN
- + VoIP**
  - + H.323
  - SIP
    - + ALG
    - + B2BUA**
    - + SIP UA
    - + SIP GW
    - + Trunking\_Group
    - + Availability
    - + Media Server
  - + Survivability
  - + Clients List
  - + Test UA
- + VPN
- + GRE

**B2BUA Trunking Configuration**

This page supports only IPv4 addressing.  
In order for changes to this page to be applied, you must click the "Submit" or "Apply Later" button at the bottom of the page

**Trunking Devices**

Name	Address	Port	Group	Username	Registration Status	Transport
ToOrigPBX	172.16.X.X	5060				UDP

*New Entry*

Name:  Model:

Address(IP/FQDN):  Use DNS SRV:

Port:  Transport:

Source FQDN:

Username:  Password:

Authenticate Registration:

**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

E.164 Country code Mapping

Name	Request URI	To	From	Contact	Refer-To	Referred-By	History-Info	P-Asserted-Identity	P-Preferred-Identity
⊗ AddPlusOne	✓	✓	✓	✓	✓	✓	✓	✓	✓
⊗ MinusPlusOne	✓	✓	✓	✓	✓	✓	✓	✓	✓

*New Entry*

Name:

	Country Code
<input type="checkbox"/> Select all headers	Australia
<input checked="" type="checkbox"/> Request URI:	Canada/USA
<input checked="" type="checkbox"/> To:	Canada/USA
<input checked="" type="checkbox"/> From:	Canada/USA
<input checked="" type="checkbox"/> Contact:	Canada/USA
<input checked="" type="checkbox"/> Refer-To:	Canada/USA
<input checked="" type="checkbox"/> Referred-By:	Canada/USA
<input checked="" type="checkbox"/> History-Info:	Canada/USA
<input checked="" type="checkbox"/> P-Asserted-Identity:	Canada/USA
<input checked="" type="checkbox"/> P-Preferred-Identity:	Canada/USA

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

E.164 Country code Mapping

Name	Request URI	To	From	Contact	Refer-To	Referred-By	History-Info	P-Asserted-Identity	P-Preferred-Identity
⊗ AddPlusOne	✓	✓	✓	✓	✓	✓	✓	✓	✓
⊗ MinusPlusOne	✓	✓	✓	✓	✓	✓	✓	✓	✓

*New Entry*

Name:

	Country Code
<input type="checkbox"/> Select all headers	Australia
<input checked="" type="checkbox"/> Request URI:	Canada/USA
<input checked="" type="checkbox"/> To:	Canada/USA
<input checked="" type="checkbox"/> From:	Canada/USA
<input checked="" type="checkbox"/> Contact:	Canada/USA
<input checked="" type="checkbox"/> Refer-To:	Canada/USA
<input checked="" type="checkbox"/> Referred-By:	Canada/USA
<input checked="" type="checkbox"/> History-Info:	Canada/USA
<input checked="" type="checkbox"/> P-Asserted-Identity:	Canada/USA
<input checked="" type="checkbox"/> P-Preferred-Identity:	Canada/USA

Figure 17: Actions - ToZoomCloud

### Actions

Name	Send	Prio	Hunt	Header	Refer-To-ReINV
ToZoomCloud	✓				
ToOrigSBC	✓				

New Entry

Name:

Send To:

- Trunking Device:
- Client:
- URI:
- Response:

Prioritize:  Refer to Re-INVITE:

Serial Hunting:  Add  Delete

E.164 Conversion rule:  Conversion mode:

Figure 18: Actions - ToOrigPBX

### Actions

Name	Send	Prio	Hunt	Header	Refer-To-ReINV
ToZoomCloud	✓				
ToOrigPBX	✓				

New Entry

Name:

Send To:

- Trunking Device:
- Client:
- URI:
- Response:

Prioritize:  Refer to Re-INVITE:

Serial Hunting:  Add  Delete

E.164 Conversion rule:  Conversion mode:

Figure 19: Match - Outbound

### Match

Direction	Mode	Def	Called		Calling		Source	Action
			Match	Pattern	Match	Pattern		
Outbound	RemoteModeOnly		matches	.			ToOrigPBX	ToZoomCloud
Inbound	RemoteModeOnly	✓					Any	ToOrigPBX

New Entry

Direction:

Mode:

default

Pattern:

Called Party:

Calling Party:

Source:

Action:

Update

Figure 20: Match - Inbound

Match								
Direction	Mode	Def	Called		Calling		Source	Action
			Match	Pattern	Match	Pattern		
Outbound	RemoteModeOnly		matches	.			ToOrigPBX	ToZoomCloud
Inbound	RemoteModeOnly	✓					Any	ToOrigPBX

New Entry

Direction: Inbound

Mode: RemoteModeOnly

default

Pattern: Called

Called Party: matches

Calling Party: matches

Source: Any

Action: ToOrigPBX

## 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

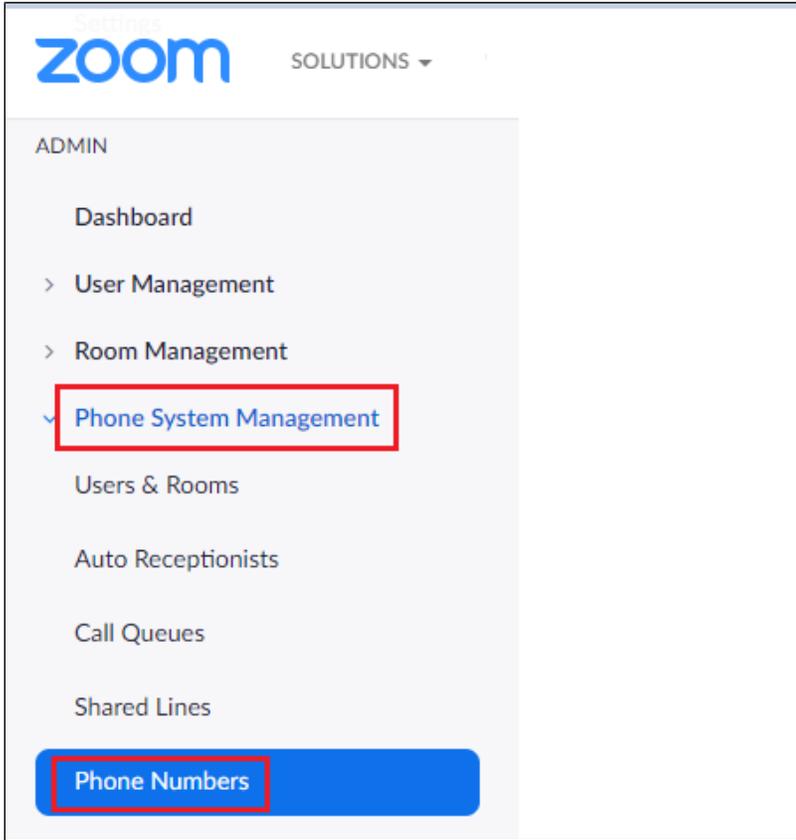
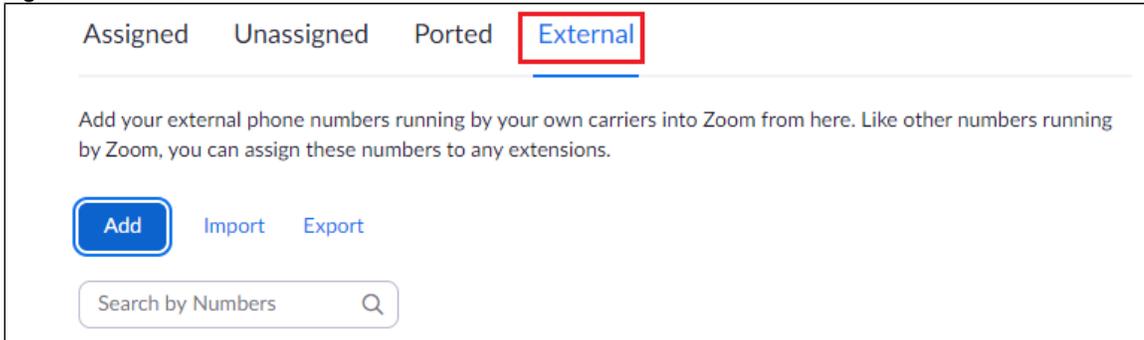


Figure 22: External



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

Figure 23: Add External Number

## Add External Numbers

Carrier **BYOC** ▼

Numbers

Example: +19991234567, +19991234568

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

**Figure 24:** External Number created successfully

Assigned Unassigned Ported **External**

Add your external phone numbers running by your own carriers into Zoom from here. Like other numbers running by Zoom, you can assign these numbers to any extensions.

Search by Numbers

Number Type (All) ▼

Number	Number Type	Carrier	Country	Submission Date
(512) 567-1233	Toll Number	BYOC	United States	May 8, 2020, 12:05 AM

## 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

zoom SOLUTIONS ▾ PLANS & PRICING CONTACT SALES SCHEDULE A MEETING JOIN A MEETING HOST A MEETING ▾

Phone Recordings Settings

ADMIN

Dashboard

> User Management

> Room Management

> **Phone System Management**

**Users & Rooms**

Search by Name, Ext. or Number

Plan (All) ▼ Status (All) ▼

Assign Numbers ▾ Assign Calling Plan ▾ Apply Settings Remove ▾

<input type="checkbox"/>	Name	Ext.	Calling Plan(s)	Number(s)	Desk Phone(s)	User Status
<input type="checkbox"/>	[REDACTED]	805	--	--	--	Active

Figure 26: Assign BYOC calling plan

### Assign BYOC Calling Plan

You are going to assign Calling Plan to the user

Users [REDACTED]

Calling Plan  BYOC Calling Plan

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

Figure 27: Choose from Unassigned Numbers

### Choose from Unassigned External Numbers

Search   Number Type (All)

<input checked="" type="checkbox"/>	Number	Location	Number Type
<input checked="" type="checkbox"/>	(512) 567-1233 <input type="button" value="E"/>	United States	Toll Number

Page Size  Total 1

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

Search by Name, Ext. or Number   Plan (All)

Assign Numbers  Assign Calling Plan  Apply Settings Remove

<input type="checkbox"/>	Name <input type="button" value="v"/>	Ext. <input type="button" value="v"/>	Calling Plan(s)	Number(s)	Desk Phone(s)	User Status
<input type="checkbox"/>	<span style="background-color: red; color: black;">[REDACTED]</span>	805	<input type="button" value="E"/> BYOC	<input type="button" value="E"/> (512) 567-1233	--	Active

## 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](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

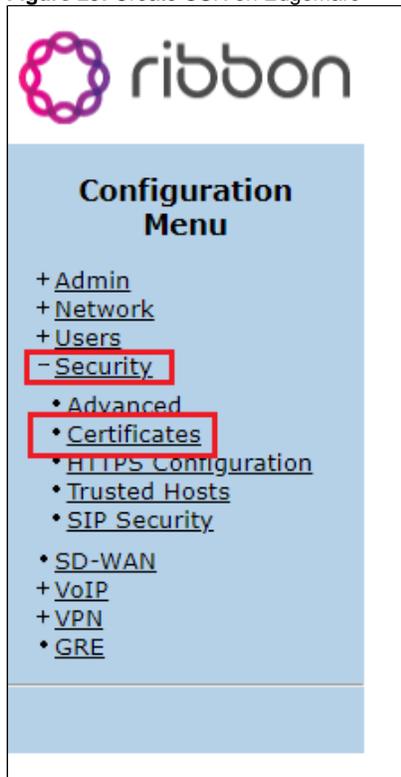
### Prerequisites:

- As the TLS needs to be 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

**Create a Certificate**

Certificate Name:

Certificate Type:

Key Size:

Certificate Authority:

Country Name (2 letter code):

State or Province (full name):

Locality Name (e.g., City):

Organization (e.g., Company):

Organization Unit:

Common Name:

Email:

*Password is optional*

Password:

Password (Verify):

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

Figure 31: Download CSR

**Certificates** [Help](#)

Certificates						
	Name	Type	CSR	Password	Certificate	Key
<input type="checkbox"/>	GoDaddyroot	CA Certificate			<a href="#">Download</a>	
<input type="checkbox"/>	SBCpem	SSL			<a href="#">Download</a>	<a href="#">Download</a>
<input type="checkbox"/>	<b>SBCCSR</b>	SSL	Y		<a href="#">Download</a>	<a href="#">Download</a>

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

**Add a Certificate**

Certificate Name:

Certificate Type:

Select Certificate File:  No file chosen

Select Key File:  No file chosen

Password:

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

**Add a Certificate**

Certificate Name:

Certificate Type:

Select Certificate File:  No file chosen

Select Key File:  No file chosen

Password:

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

**Figure 34:** SIP Settings

[Help](#)

## SIP Settings

SIP protocol settings.

---

The SIP Server settings specify the address and port that all client traffic shall be forwarded to.

SIP Server Address:

SIP Server Port:

SIP Server Transport:

Enable SRTP:

Use Custom Domain:

SIP Server Domain:

List of SIP Servers:

Enable Multi-homed Outbound Proxy Mode:

Enable Transparent Proxy Mode:

Limit Outbound to listed SIP Servers:

Limit Inbound to listed SIP Servers:

Include UPDATE In Allow:

PRACK Support:

GEOLOCATION Support:

Call Audit Support:

---

**B2BUA Options:**

B2BUA Redirect Support (302):

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

**Figure 35:** TLS cipher and WAN certificate

**TLS**

Port:

TLS Protocol:

Ciphers String:

VLAN 1: Certificate:  Policy:

WAN: Certificate:  Policy:

Exclude sips headers for TLS Transport:

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

**Figure 36:** SRTP config

**Media Security:**

Enable SRTP support:

Enable MKI support: