zoomphone

Configuration Guide For Avaya SBC

Document version 1.1

Table of Contents

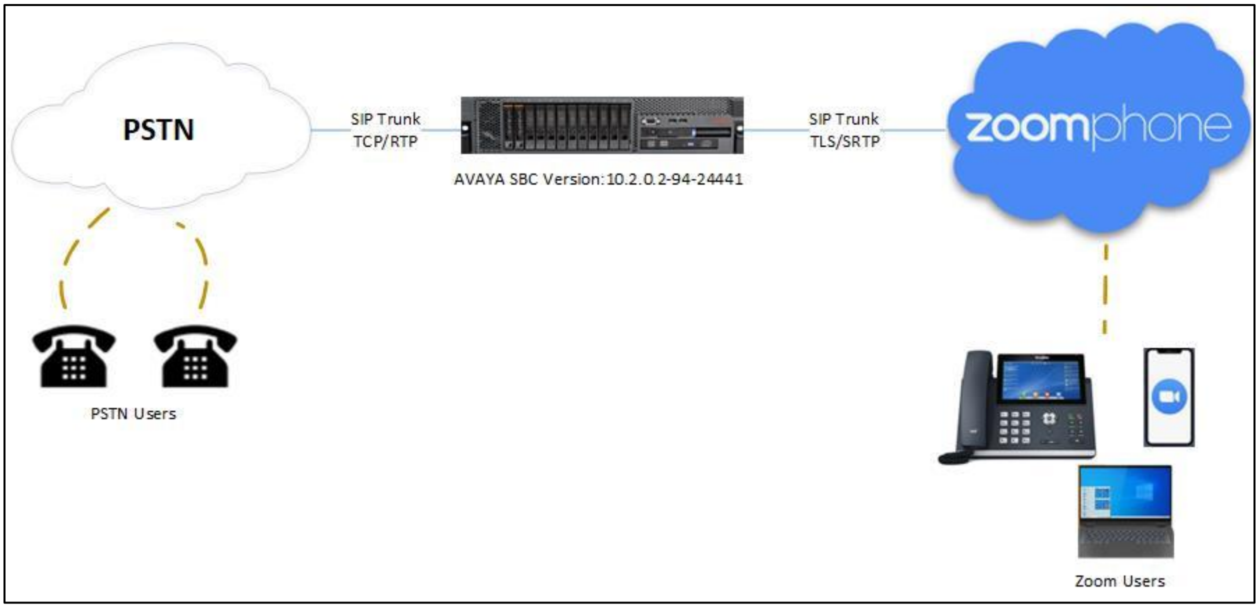
Revision History

Version	Date	Author	Change
1.0	10-August-2020	Zoom	Template design
1.1	4-December-2024	Rajesh Kannan	Updated document for Avaya SBC configurations

1 Overview

This document provides instructions on how to configure and add your device to the Zoom web portal. This document provides instructions on how to set up **Avaya Session Border Controller** (hereafter, referred to as SBC) for interoperability between Generic SIP Trunk and Zoom Phone environment.

2 Topology

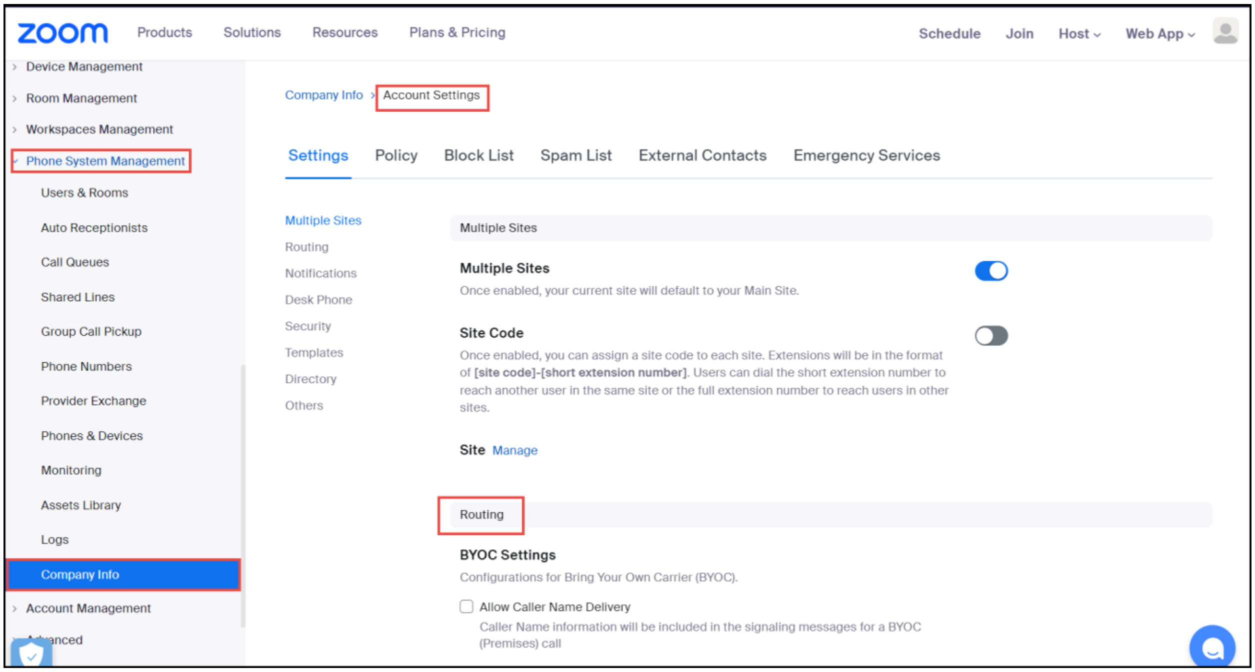


3 Configuration Steps- ZOOM PBX

This section covers checking the basic readiness, adding the external BYOC DID phone numbers and mapping them to corresponding end point devices (such as IP phones and other SIP devices).

3.1 Adding Your SBC

- Login to Zoom Admin Portal and Navigate to **Phone System Management->Company Info->Account Settings->Routing**



Multiple Sites

Multiple Sites

Once enabled, your current site will default to your Main Site.

Site Code

Once enabled, you can assign a site code to each site. Extensions will be in the format of **[site code]-[short extension number]**. Users can dial the short extension number to reach another user in the same site or the full extension number to reach users in other sites.

Site Manage

Routing

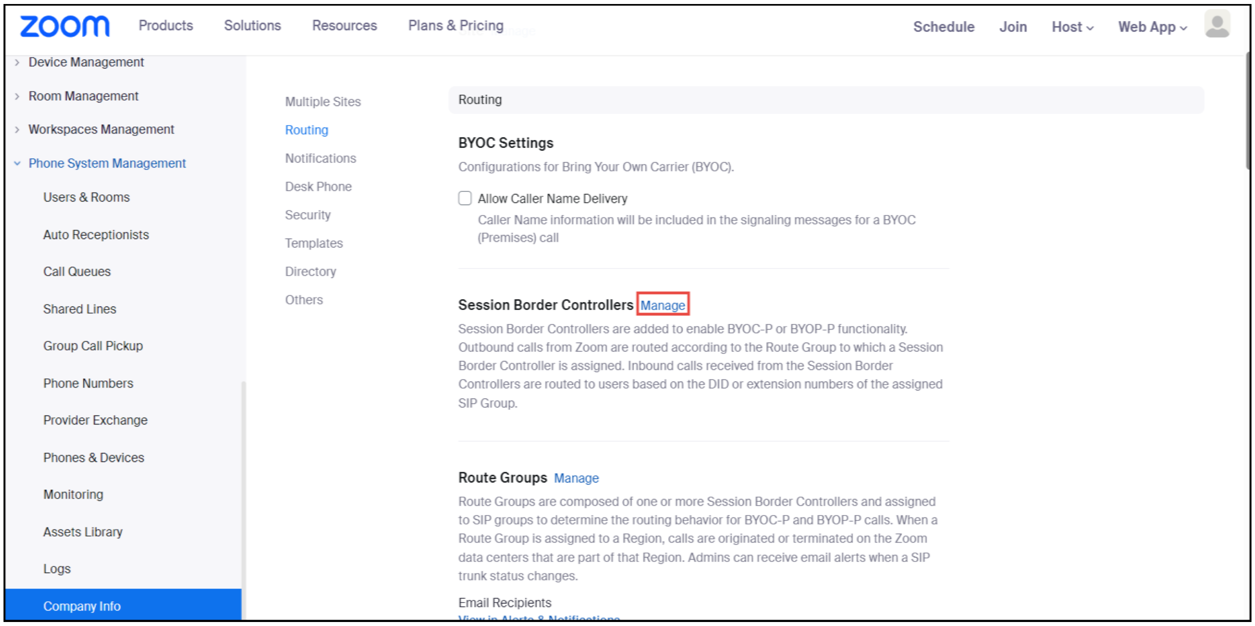
BYOC Settings

Configurations for Bring Your Own Carrier (BYOC).

☐ Allow Caller Name Delivery

Caller Name information will be included in the signaling messages for a BYOC (Premises) call

- To add your SBC, locate **Session Border Controllers** and click on **Manage**



Routing

BYOC Settings

Configurations for Bring Your Own Carrier (BYOC).

☐ Allow Caller Name Delivery

Caller Name information will be included in the signaling messages for a BYOC (Premises) call

Session Border Controllers Manage

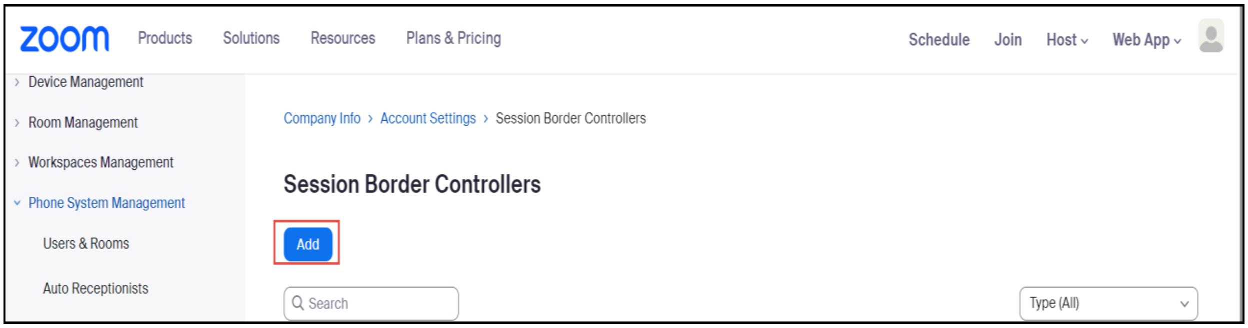
Session Border Controllers are added to enable BYOC-P or BYOP-P functionality. Outbound calls from Zoom are routed according to the Route Group to which a Session Border Controller is assigned. Inbound calls received from the Session Border Controllers are routed to users based on the DID or extension numbers of the assigned SIP Group.

Route Groups Manage

Route Groups are composed of one or more Session Border Controllers and assigned to SIP groups to determine the routing behavior for BYOC-P and BYOP-P calls. When a Route Group is assigned to a Region, calls are originated or terminated on the Zoom data centers that are part of that Region. Admins can receive email alerts when a SIP trunk status changes.

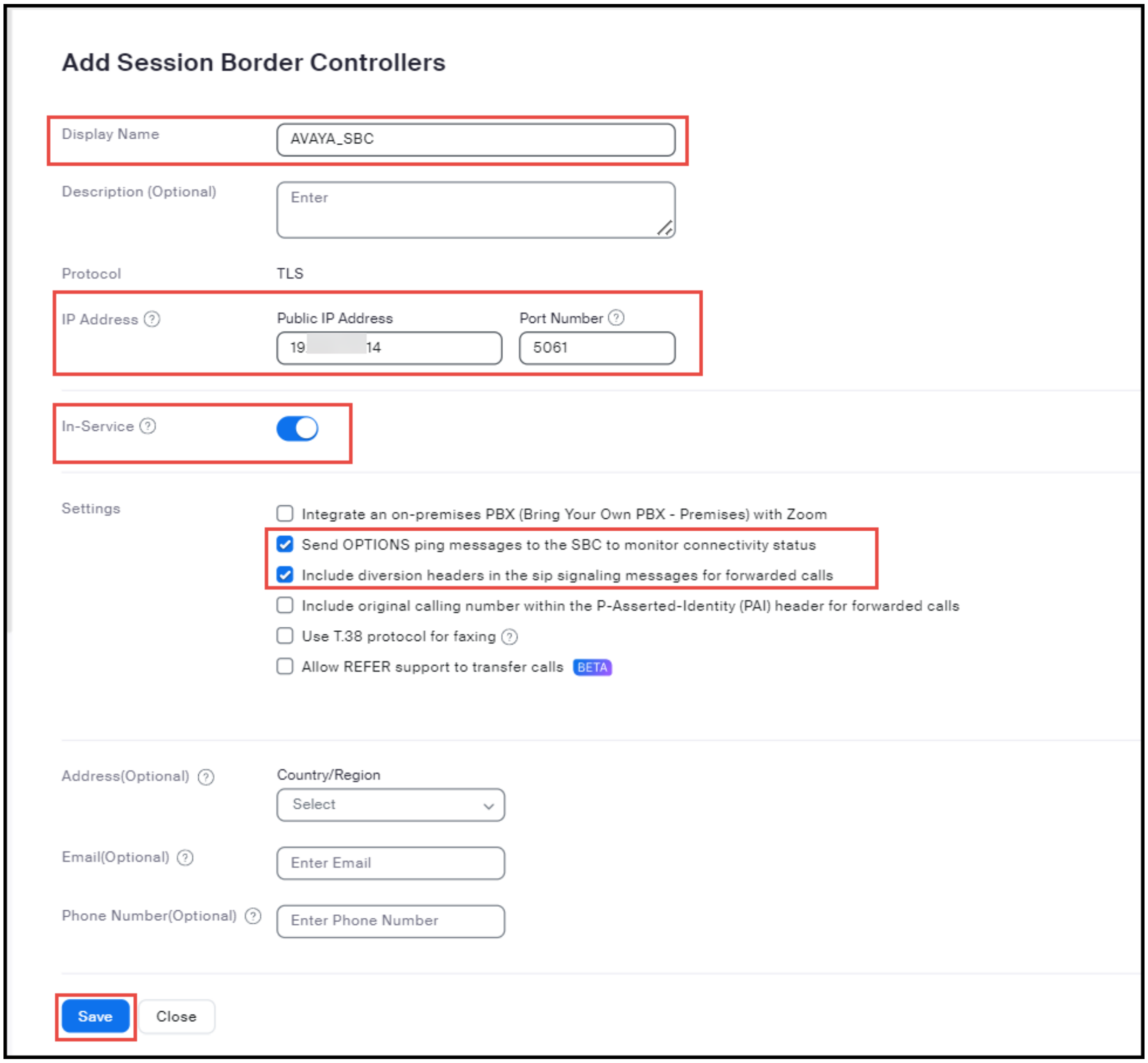
Email Recipients

- Click on **Add**



Session Border Controllers

- **Display Name:** Provide the Display name of your choice. Here, AVAYA_SBC is used
- **IP Address:** Provide the IP address AVAYA SBC interface facing towards Zoom and configure the port number
- **In-Service:** Enabled
- **Settings:** Check “Send OPTIONS ping messages to the SBC to monitor connectivity status” and “Include diversion headers in the sip signaling messages for forwarded calls”
- Click **Save**



Add Session Border Controllers

Display Name: AVAYA_SBC

Description (Optional): Enter

Protocol: TLS

IP Address ⓘ — Public IP Address: 19[redacted]14 — Port Number ⓘ: 5061

In-Service ⓘ: ●

Settings:
- ☐ Integrate an on-premises PBX (Bring Your Own PBX - Premises) with Zoom
- ☑ Send OPTIONS ping messages to the SBC to monitor connectivity status
- ☑ Include diversion headers in the sip signaling messages for forwarded calls
- ☐ Include original calling number within the P-Asserted-Identity (PAI) header for forwarded calls
- ☐ Use T.38 protocol for faxing ⓘ
- ☐ Allow REFER support to transfer calls BETA

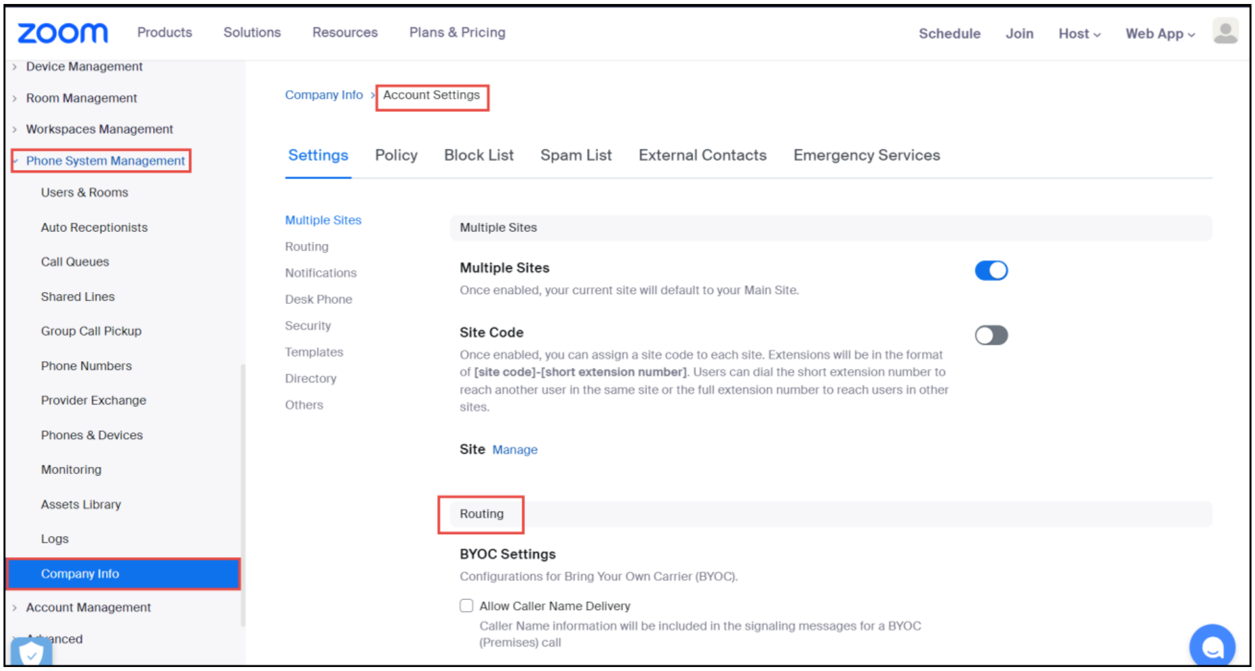
Address(Optional) ⓘ — Country/Region: Select

Email(Optional) ⓘ: Enter Email

Phone Number(Optional) ⓘ: Enter Phone Number

3.2 Adding Route Group

- Navigate to **Phone System Management -> Company Info -> Account Settings -> Routing**



Multiple Sites

Multiple Sites
Once enabled, your current site will default to your Main Site.

Site Code
Once enabled, you can assign a site code to each site. Extensions will be in the format of **[site code]-[short extension number]**. Users can dial the short extension number to reach another user in the same site or the full extension number to reach users in other sites.

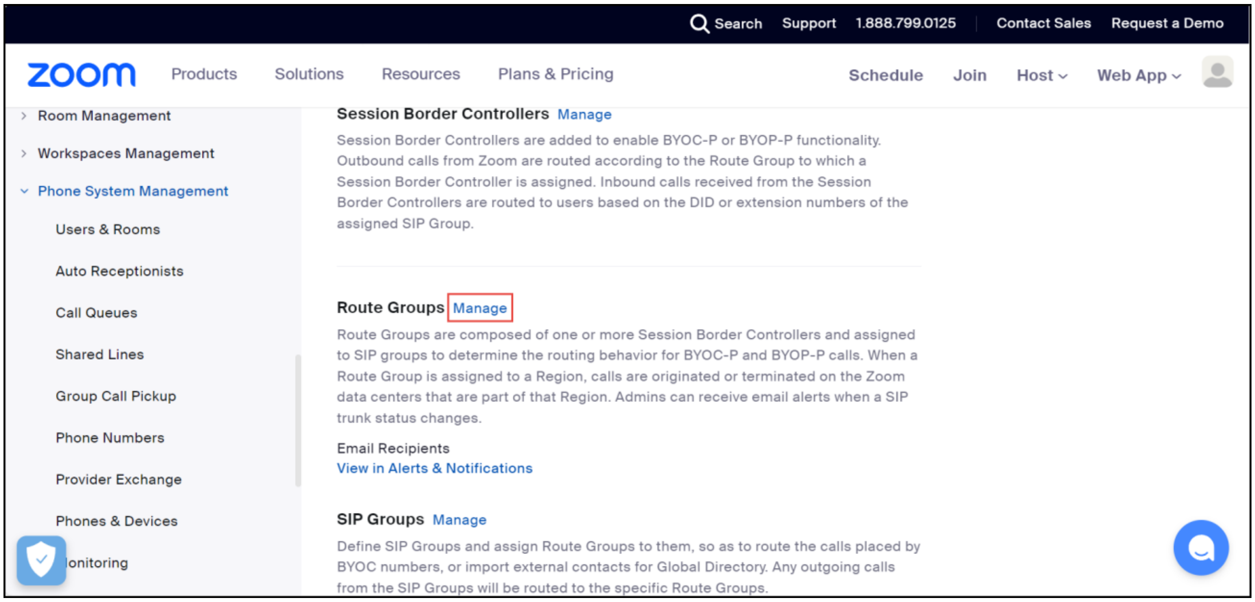
Site Manage

Routing

BYOC Settings
Configurations for Bring Your Own Carrier (BYOC).

☐ Allow Caller Name Delivery
Caller Name information will be included in the signaling messages for a BYOC (Premises) call

- To add the Route Groups, locate **Route Groups** and click on **Manage**



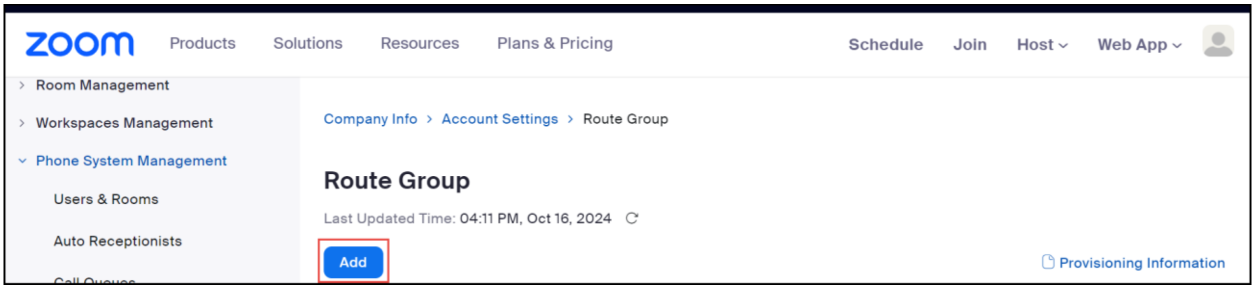
Session Border Controllers Manage
Session Border Controllers are added to enable BYOC-P or BYOP-P functionality. Outbound calls from Zoom are routed according to the Route Group to which a Session Border Controller is assigned. Inbound calls received from the Session Border Controllers are routed to users based on the DID or extension numbers of the assigned SIP Group.

Route Groups Manage
Route Groups are composed of one or more Session Border Controllers and assigned to SIP groups to determine the routing behavior for BYOC-P and BYOP-P calls. When a Route Group is assigned to a Region, calls are originated or terminated on the Zoom data centers that are part of that Region. Admins can receive email alerts when a SIP trunk status changes.

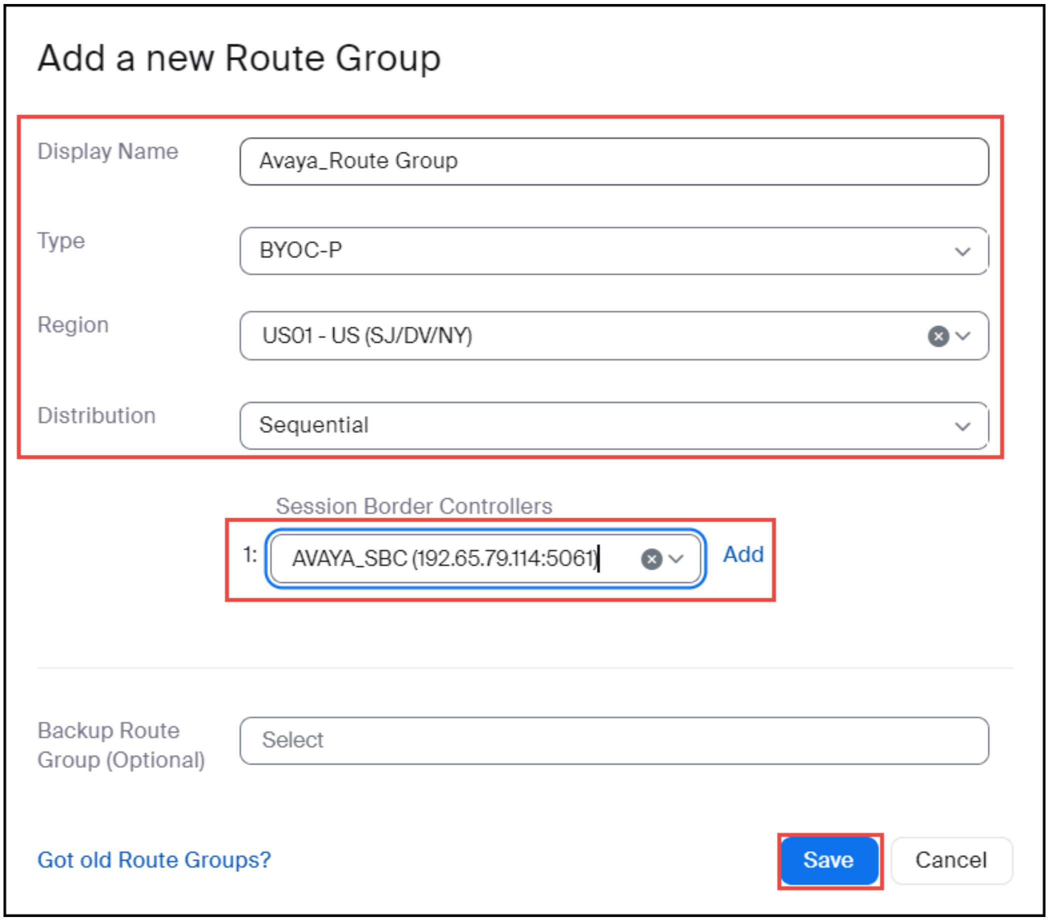
Email Recipients
View in Alerts & Notifications

SIP Groups Manage
Define SIP Groups and assign Route Groups to them, so as to route the calls placed by BYOC numbers, or import external contacts for Global Directory. Any outgoing calls from the SIP Groups will be routed to the specific Route Groups.

- Click on **Add**



- **Display Name:** Provide the display name of your choice. Here, Avaya_Route Group is used
- **Type:** Select BYOC-P
- **Region:** Select "US01-US(SJ/DV/NY)"
- **Distribution:** Select Sequential from the dropdown and then add Avaya_SBC that was created in the above step
- Click **Save**



Add a new Route Group

Display Name: Avaya_Route Group

Type: BYOC-P

Region: US01 - US (SJ/DV/NY)

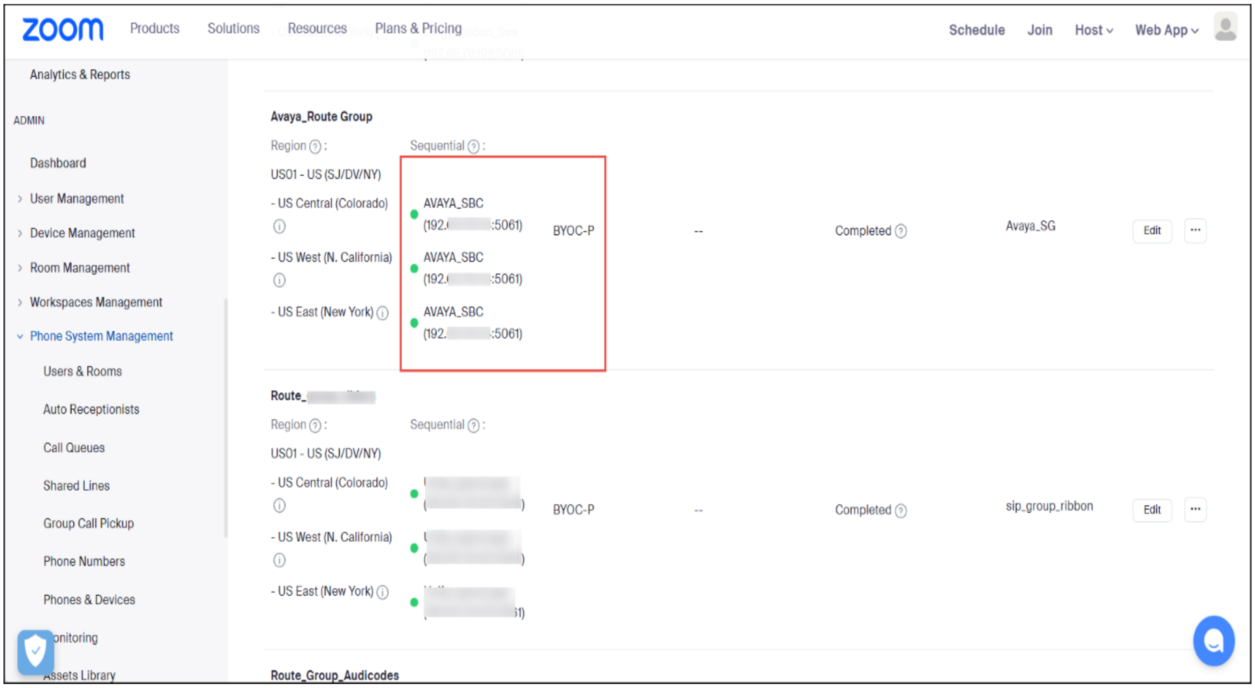
Distribution: Sequential

Session Border Controllers

1: AVAYA_SBC (192.65.79.114:5061)

Backup Route Group (Optional): Select

- A green led indicates the trunk status is active as shown in screenshot below



Avaya_Route Group

Region ⓘ: Sequential ⓘ:

US01 - US (SJ/DV/NY)

- US Central (Colorado) ⓘ ● AVAYA_SBC (192.[redacted]:5061) BYOC-P -- Completed ⓘ Avaya_SG Edit ···
- US West (N. California) ⓘ ● AVAYA_SBC (192.[redacted]:5061)
- US East (New York) ⓘ ● AVAYA_SBC (192.[redacted]:5061)

Route_[redacted]

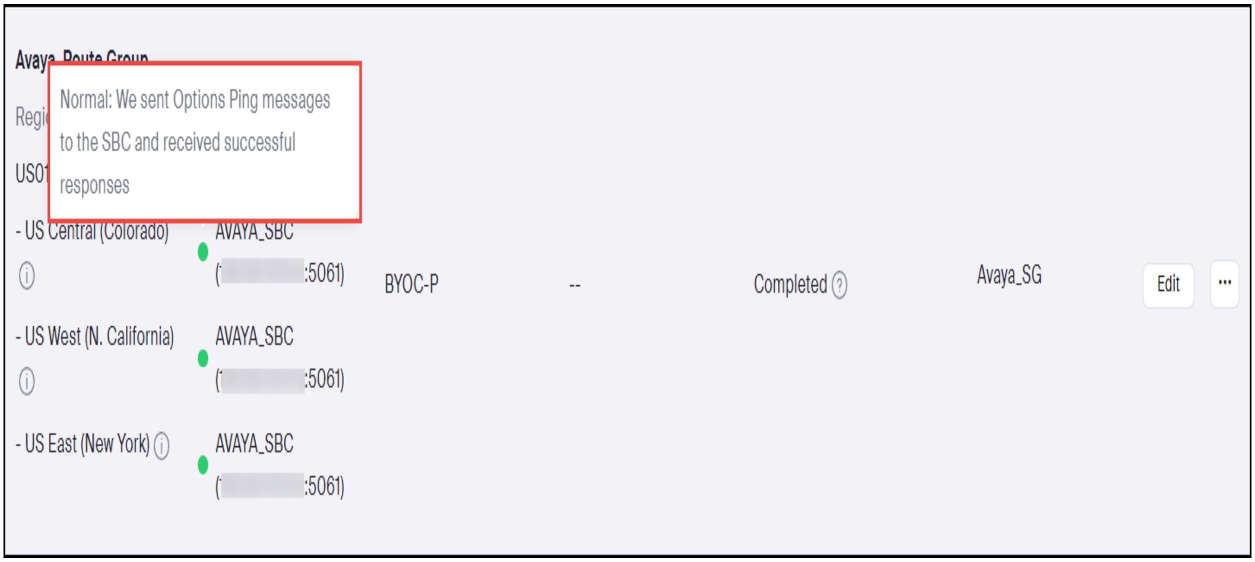
Region ⓘ: Sequential ⓘ:

US01 - US (SJ/DV/NY)

- US Central (Colorado) ⓘ ● [redacted] BYOC-P -- Completed ⓘ sip_group_ribbon Edit ···
- US West (N. California) ⓘ ● [redacted]
- US East (New York) ⓘ ● [redacted]

Route_Group_Audicodes

- Moving the cursor towards green led shows the trunk status as shown in screenshot below



Avaya_Route Group

Normal: We sent Options Ping messages to the SBC and received successful responses

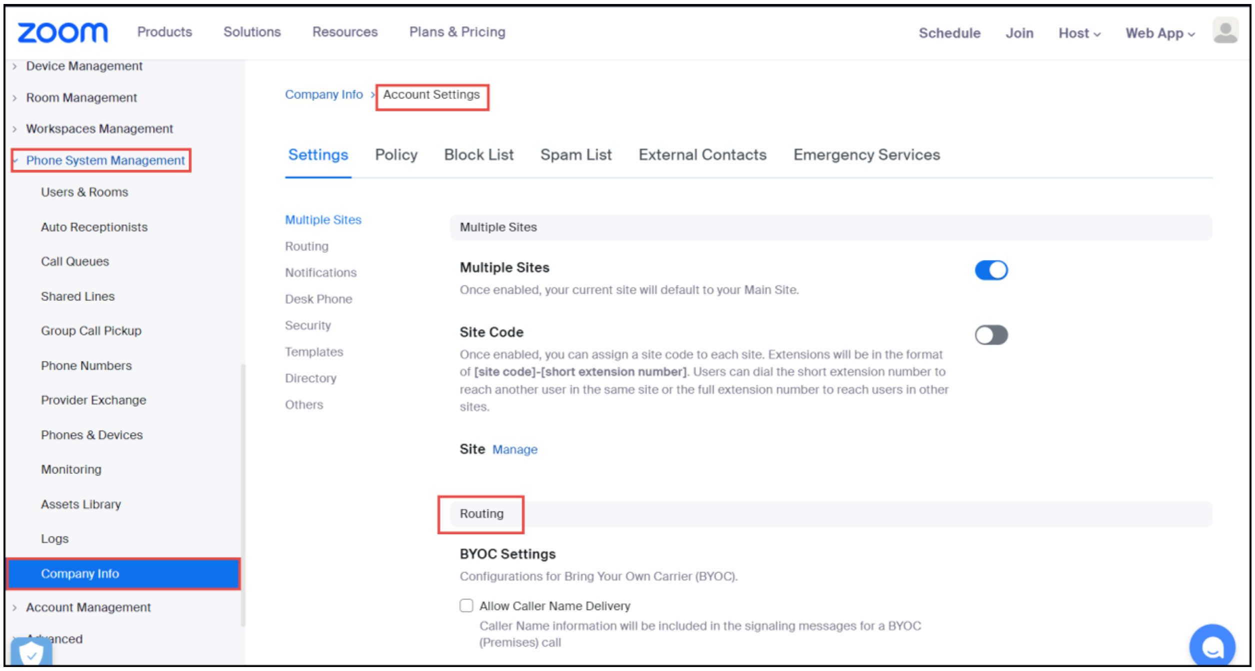
Regi

US01

- US Central (Colorado) ⓘ ● AVAYA_SBC ([redacted]:5061) BYOC-P -- Completed ⓘ Avaya_SG Edit ···
- US West (N. California) ⓘ ● AVAYA_SBC ([redacted]:5061)
- US East (New York) ⓘ ● AVAYA_SBC ([redacted]:5061)

3.3 Adding SIP Group

- Navigate to **Phone System Management -> Company Info -> Account Settings -> Routing**



Multiple Sites

Once enabled, your current site will default to your Main Site.

Site Code

Once enabled, you can assign a site code to each site. Extensions will be in the format of **[site code]-[short extension number]**. Users can dial the short extension number to reach another user in the same site or the full extension number to reach users in other sites.

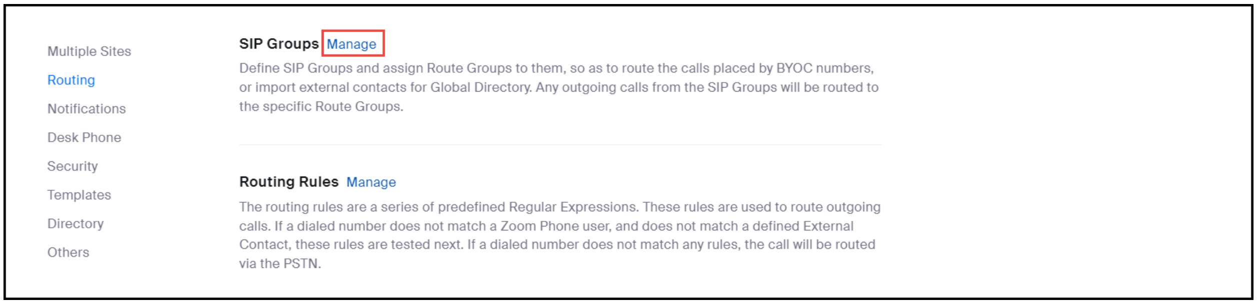
BYOC Settings

Configurations for Bring Your Own Carrier (BYOC).

□ Allow Caller Name Delivery

Caller Name information will be included in the signaling messages for a BYOC (Premises) call

- To add the SIP Groups, locate **SIP Groups** and click on **Manage**



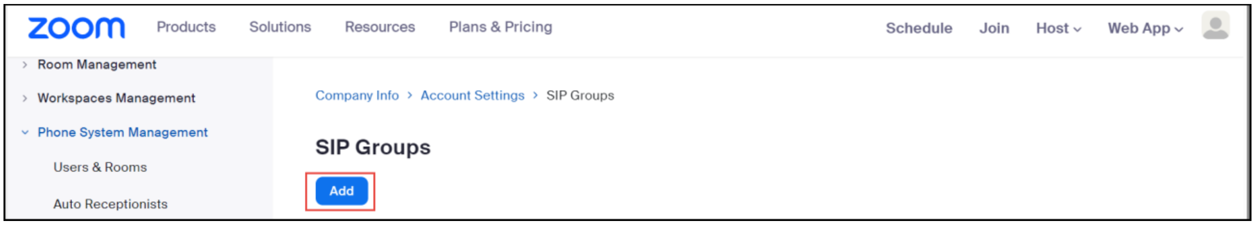
SIP Groups Manage

Define SIP Groups and assign Route Groups to them, so as to route the calls placed by BYOC numbers, or import external contacts for Global Directory. Any outgoing calls from the SIP Groups will be routed to the specific Route Groups.

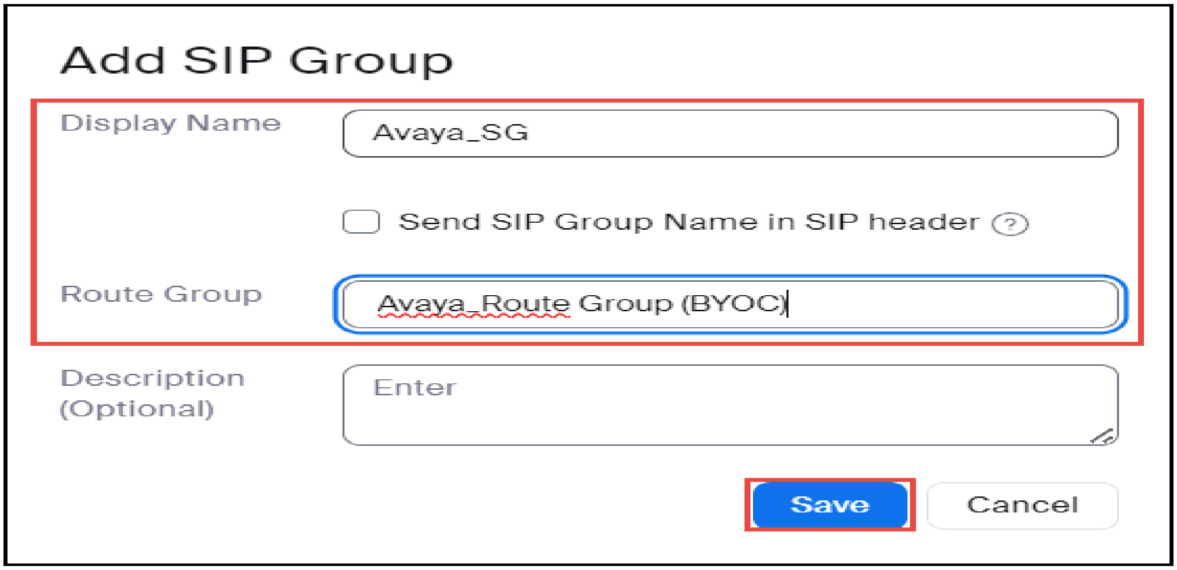
Routing Rules Manage

The routing rules are a series of predefined Regular Expressions. These rules are used to route outgoing calls. If a dialed number does not match a Zoom Phone user, and does not match a defined External Contact, these rules are tested next. If a dialed number does not match any rules, the call will be routed via the PSTN.

- Click on **Add**



- **Display Name:** Provide display name of your choice. Here Avaya_SG is used
- **Route Group:** Select Avaya_Route Group (BYOC) from the drop down
- Click **Save**



Add SIP Group

Display Name: Avaya_SG

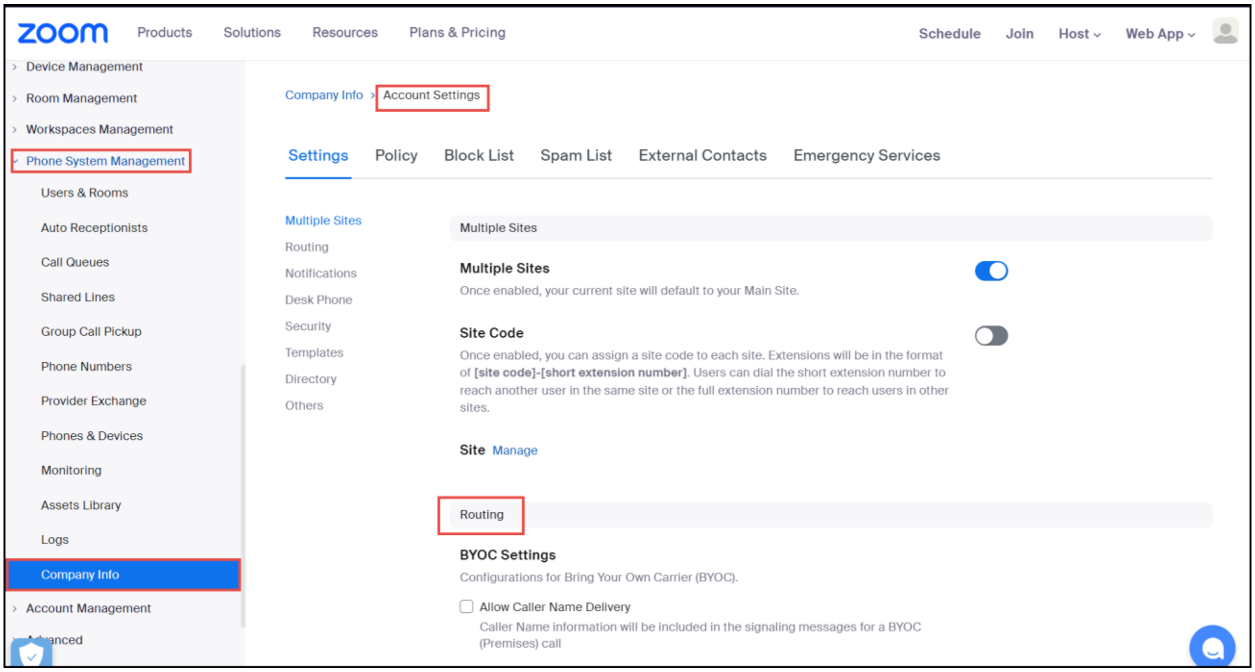
□ Send SIP Group Name in SIP header ?

Route Group: Avaya_Route Group (BYOC)

Description (Optional): Enter

3.4 Adding Routing Rule

- To add the Routing Rule, Navigate to **Phone System Management -> Company Info -> Account Settings -> Routing**



Multiple Sites

Multiple Sites
Once enabled, your current site will default to your Main Site.

Site Code
Once enabled, you can assign a site code to each site. Extensions will be in the format of **[site code]-[short extension number]**. Users can dial the short extension number to reach another user in the same site or the full extension number to reach users in other sites.

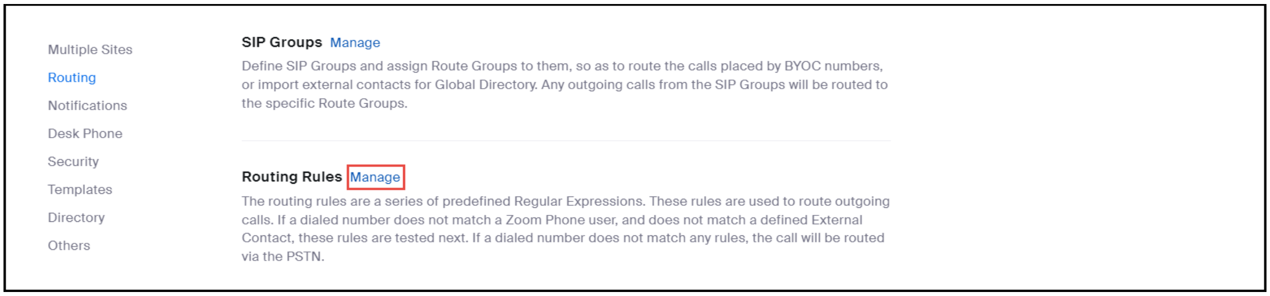
Site Manage

Routing

BYOC Settings
Configurations for Bring Your Own Carrier (BYOC).

□ Allow Caller Name Delivery
Caller Name information will be included in the signaling messages for a BYOC (Premises) call

- Locate **Routing Rules** and click on **Manage**



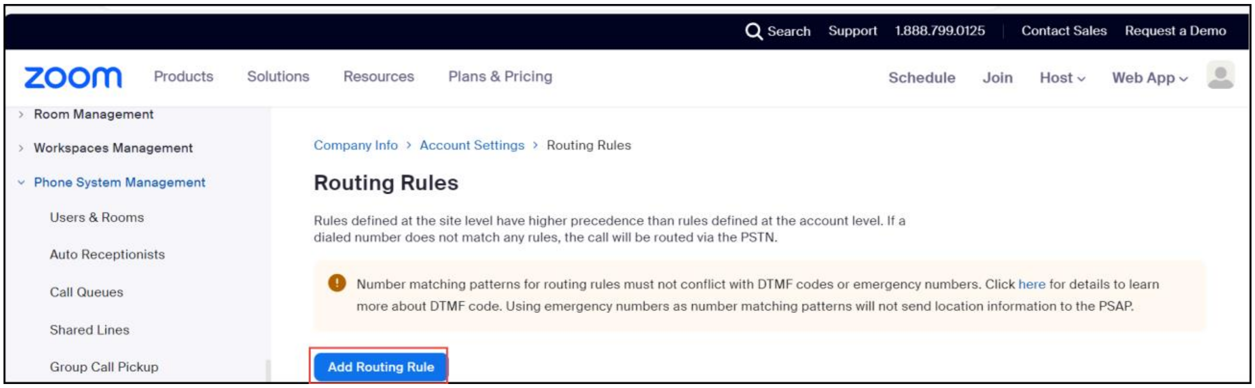
SIP Groups Manage

Define SIP Groups and assign Route Groups to them, so as to route the calls placed by BYOC numbers, or import external contacts for Global Directory. Any outgoing calls from the SIP Groups will be routed to the specific Route Groups.

Routing Rules Manage

The routing rules are a series of predefined Regular Expressions. These rules are used to route outgoing calls. If a dialed number does not match a Zoom Phone user, and does not match a defined External Contact, these rules are tested next. If a dialed number does not match any rules, the call will be routed via the PSTN.

- Click **Add Routing Rule** to add your rule for outbound calls

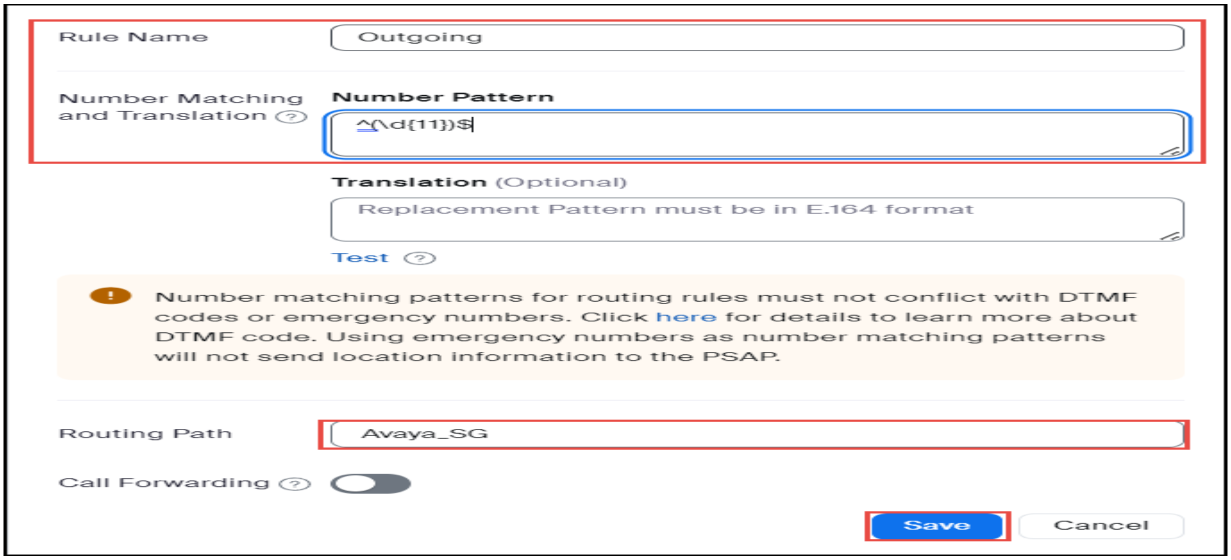


Routing Rules

Rules defined at the site level have higher precedence than rules defined at the account level. If a dialed number does not match any rules, the call will be routed via the PSTN.

Number matching patterns for routing rules must not conflict with DTMF codes or emergency numbers. Click here for details to learn more about DTMF code. Using emergency numbers as number matching patterns will not send location information to the PSAP.

- **Rule Name:** Provide Rule Name as per your choice. Here Outgoing is used
- **Number Matching and Translation:** Provide the Number Pattern as given below in the screenshot and select the **Routing path** as "Avaya_SG" which was created before
- Click on **Save**



Rule Name: Outgoing

Number Matching and Translation

Number Pattern: ^(\d{11})$

Translation (Optional): Replacement Pattern must be in E.164 format

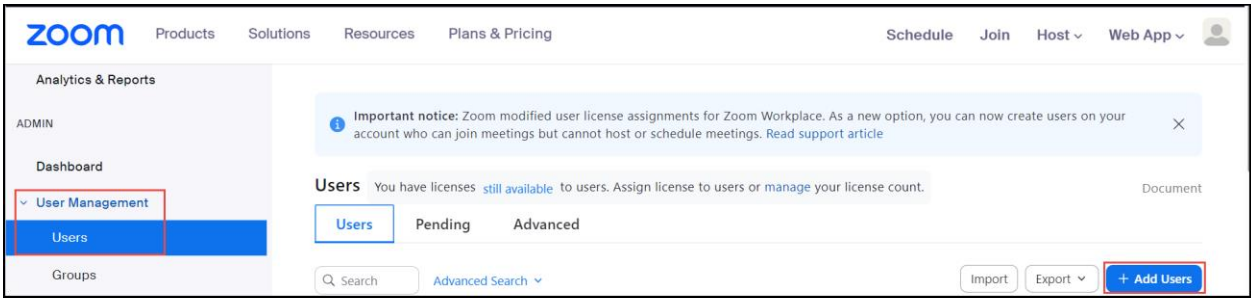
Number matching patterns for routing rules must not conflict with DTMF codes or emergency numbers. Click here for details to learn more about DTMF code. Using emergency numbers as number matching patterns will not send location information to the PSAP.

Routing Path: Avaya_SG

Call Forwarding ○

3.5 Adding Phone Users

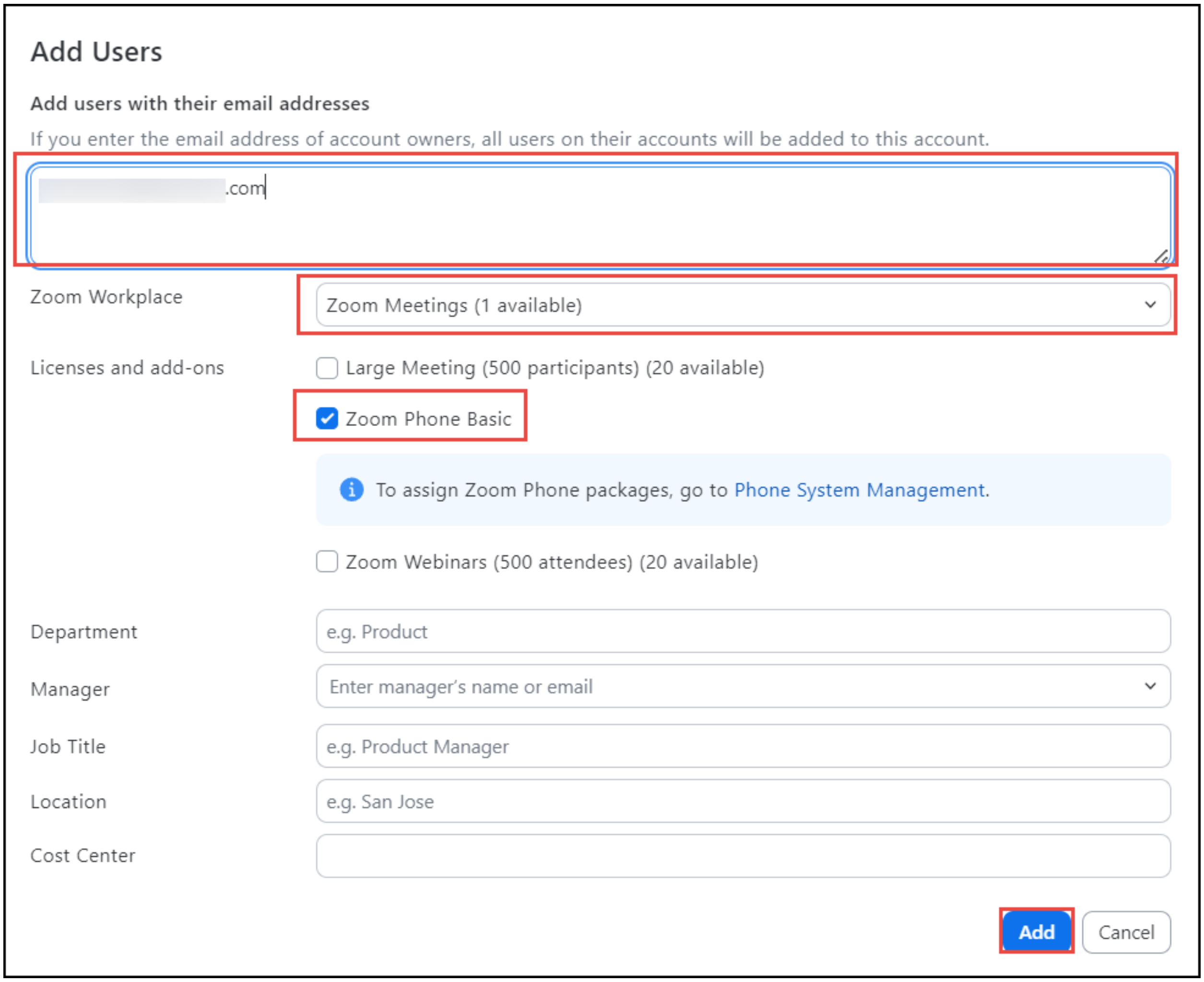
- Navigate to **User Management-> Users-> Add Users** for adding new users



Important notice: Zoom modified user license assignments for Zoom Workplace. As a new option, you can now create users on your account who can join meetings but cannot host or schedule meetings. Read support article

Users You have licenses still available to users. Assign license to users or manage your license count.

- Enter the user **email address**
- **Zoom Workplace**: choose Zoom Workplace as "**Zoom Meetings**" from the dropdown
- In "**License and add-ons**", select the checkbox "**Zoom Phone Basic**"
- Click on **Add**



Add Users

Add users with their email addresses

If you enter the email address of account owners, all users on their accounts will be added to this account.

[redacted].com

Zoom Workplace: Zoom Meetings (1 available)

Licenses and add-ons:
☐ Large Meeting (500 participants) (20 available)
☑ Zoom Phone Basic
To assign Zoom Phone packages, go to Phone System Management.
☐ Zoom Webinars (500 attendees) (20 available)

Department: e.g. Product

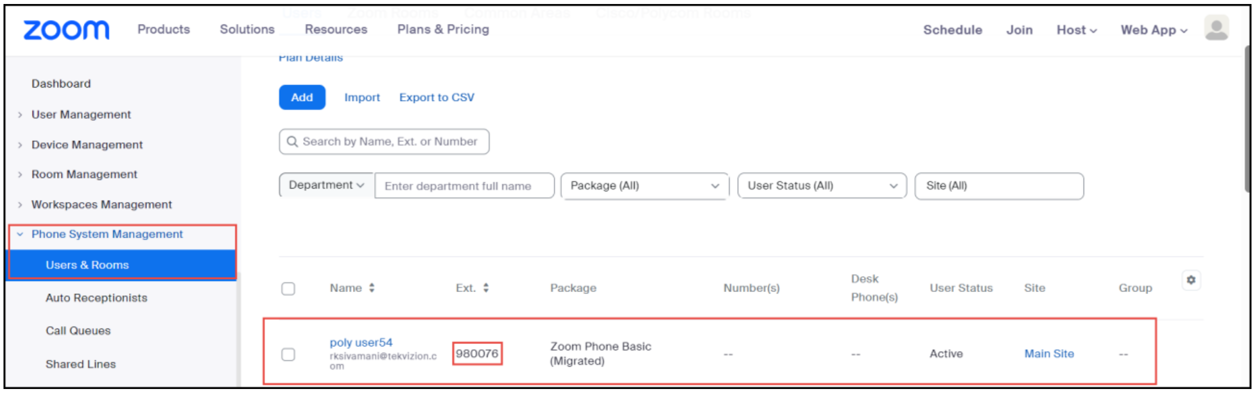
Manager: Enter manager's name or email

Job Title: e.g. Product Manager

Location: e.g. San Jose

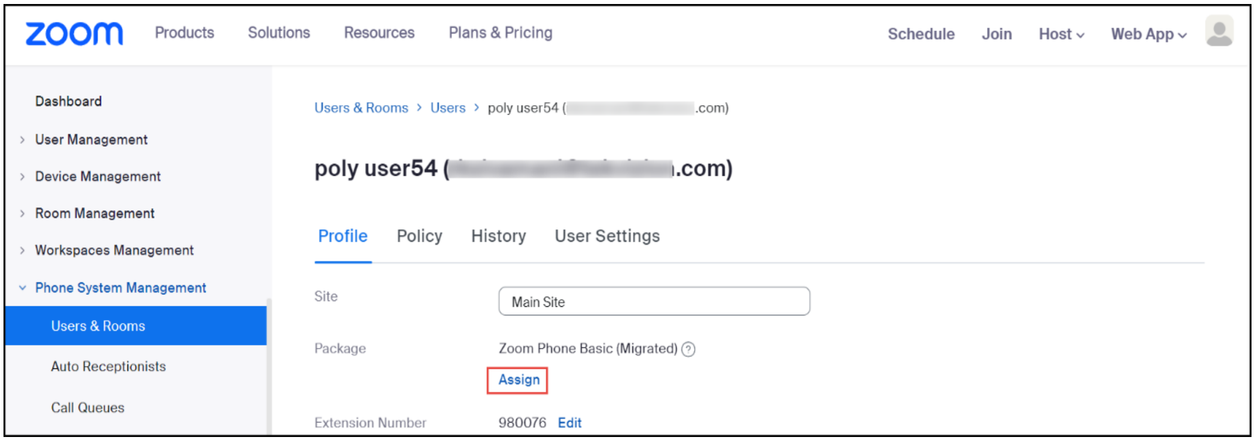
Cost Center:

- Add Calling Plan package to the user. When Zoom Phone license is assigned for a user, an extension number gets assigned to the user automatically. Navigate to **Phone System Management -> Users & Rooms.** To assign a calling plan package to the user, click on the **user** that has been created



Name	Ext.	Package	Number(s)	Desk Phone(s)	User Status	Site	Group
poly user54 rksivamani@tekvizion.com	980076	Zoom Phone Basic (Migrated)	--	--	Active	Main Site	--

- Click on **Assign**



Users & Rooms > Users > poly user54 ([redacted].com)

poly user54 ([redacted].com)

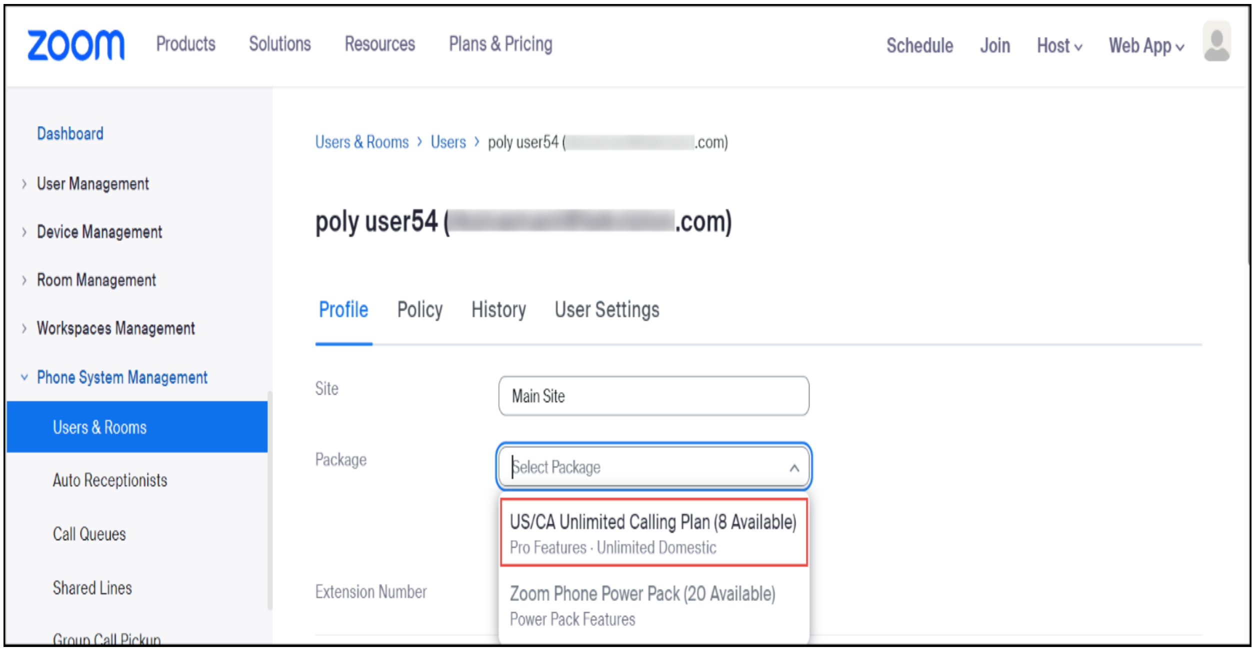
Site: Main Site

Package: Zoom Phone Basic (Migrated)

Assign

Extension Number: 980076 Edit

- Select **US/CA Unlimited Calling Plan** as shown in below screenshot



Users & Rooms › Users › poly user54 ([redacted].com)

poly user54 ([redacted].com)

Site: Main Site

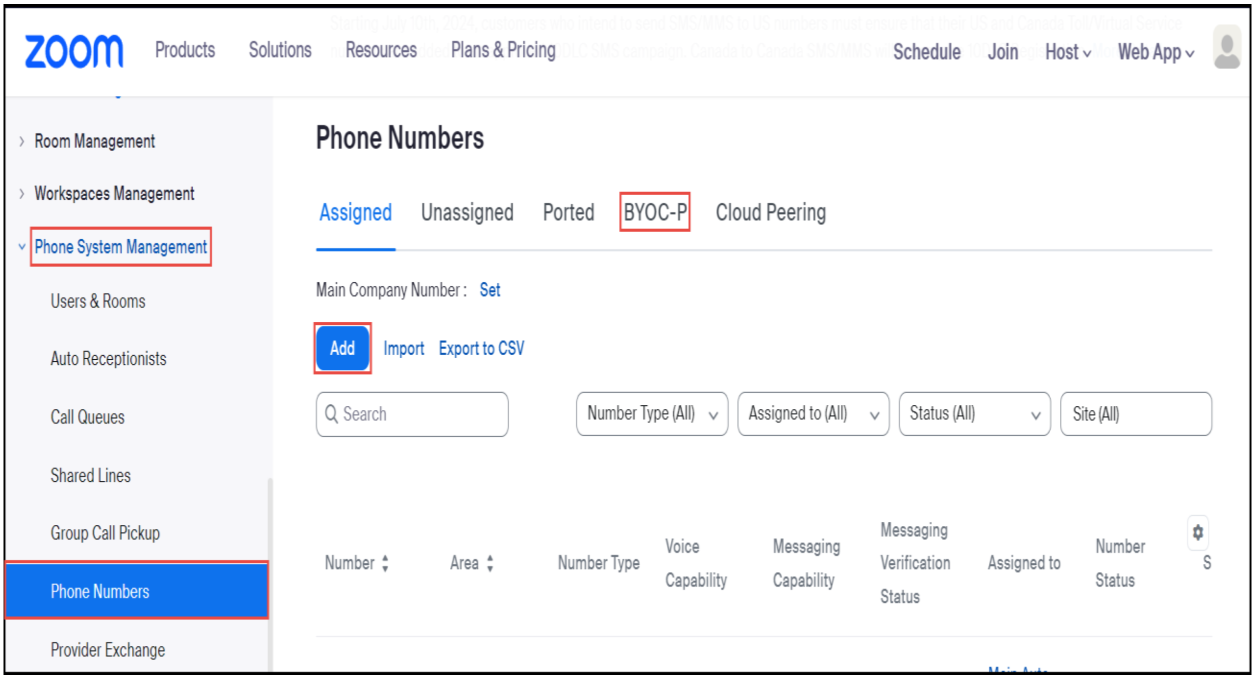
Package: Select Package

- US/CA Unlimited Calling Plan (8 Available) — Pro Features · Unlimited Domestic
- Zoom Phone Power Pack (20 Available) — Power Pack Features

Extension Number

3.6 Adding Phone Numbers

- Add the BYOC phone numbers as shown below. Navigate to **Phone System Management -> Phone Numbers-> BYOC-P->**Click **Add**

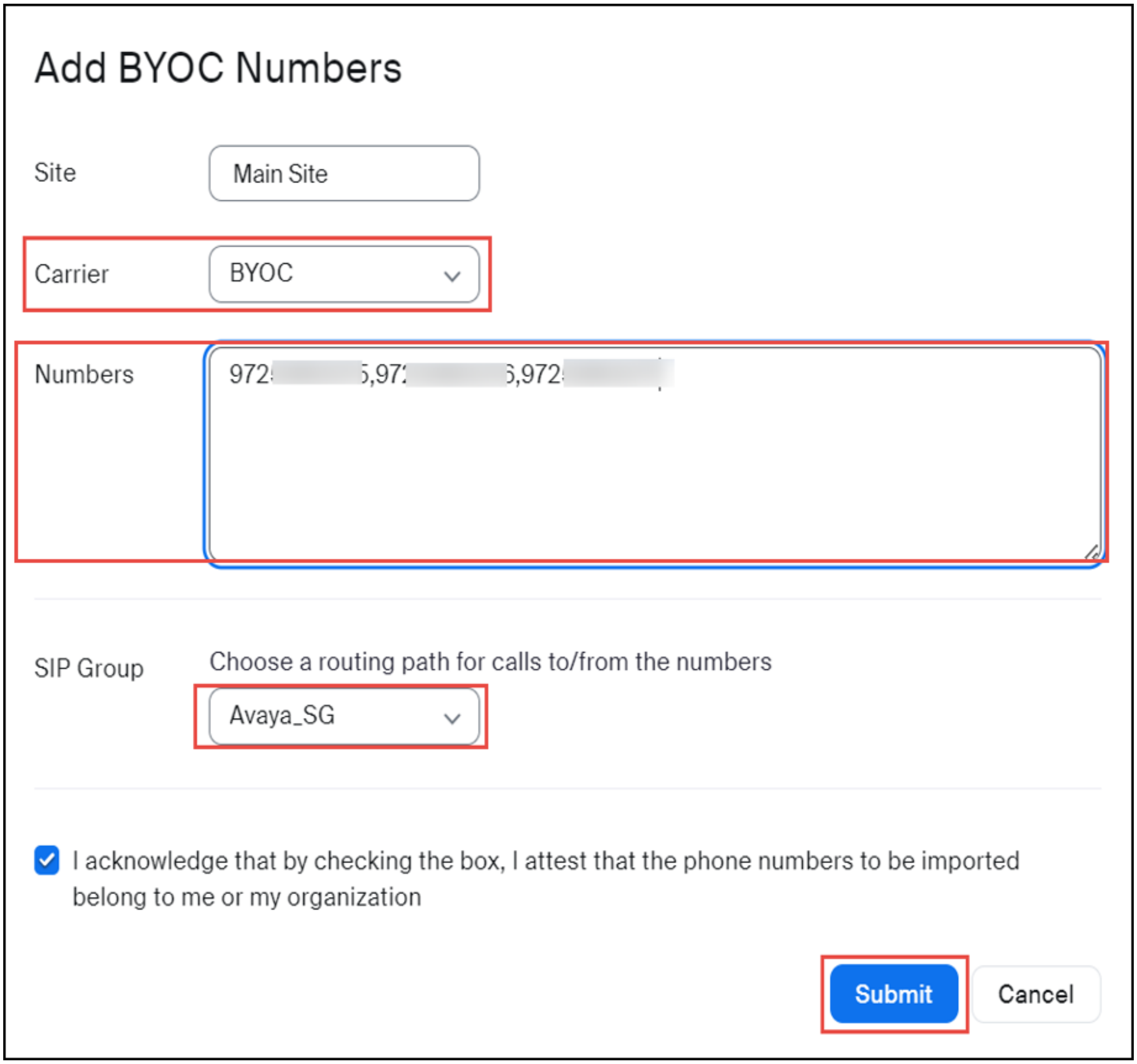


Phone Numbers

Main Company Number : Set

Number	Area	Number Type	Voice Capability	Messaging Capability	Messaging Verification Status	Assigned to	Number Status	S

- **Carrier:** BYOC
- **Numbers:** Enter the phone numbers as shown in screenshot below
- **SIP Group:** Select the SIP Group “Avaya_SG” which was created before
- Check the **acknowledgement** box and Click on **Submit**



Add BYOC Numbers

Site: Main Site

Carrier: BYOC

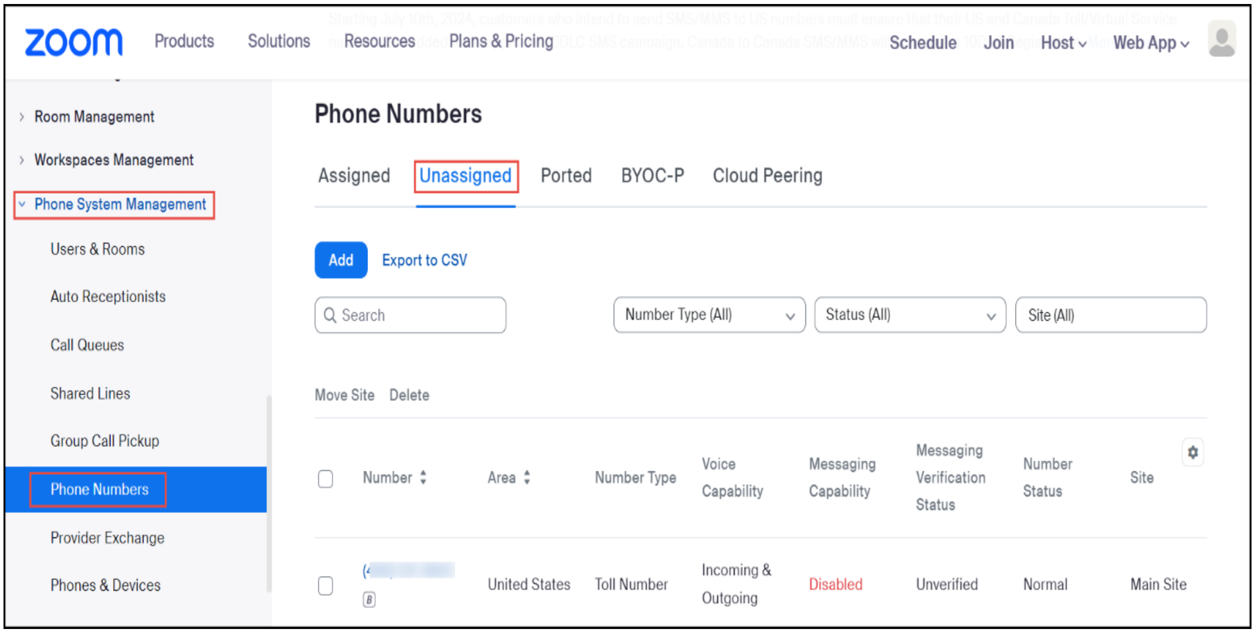
Numbers: 972[redacted]5,972[redacted]6,972[redacted]

SIP Group: Choose a routing path for calls to/from the numbers

Avaya_SG

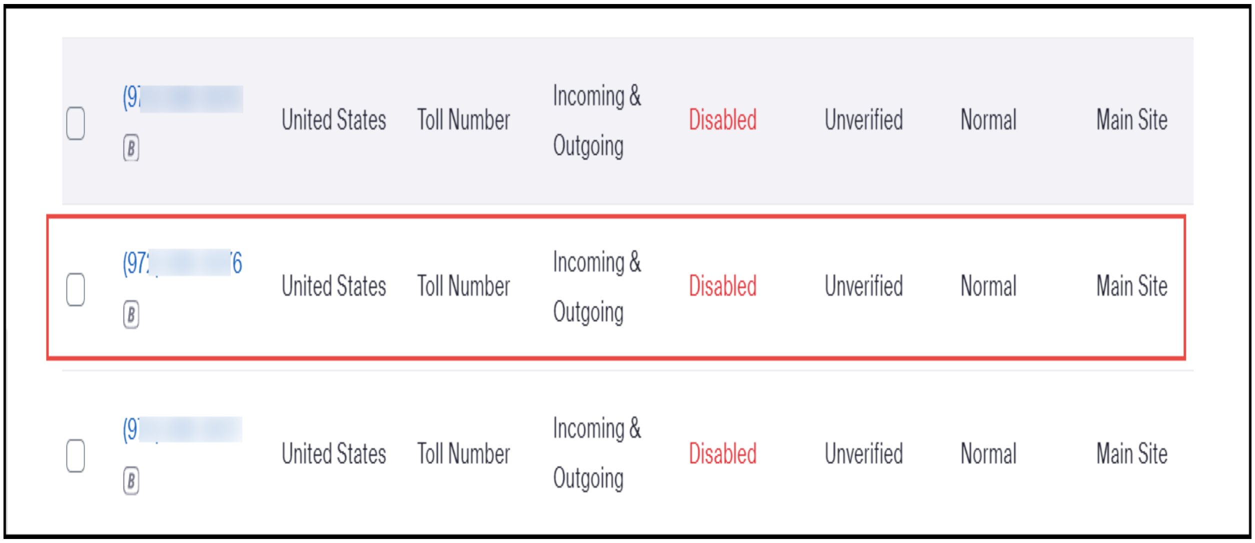
☑ I acknowledge that by checking the box, I attest that the phone numbers to be imported belong to me or my organization

- Assign the BYOC numbers to the Zoom phone users as shown below. Navigate to **Phone System Management -> Phone Numbers-> Unassigned**



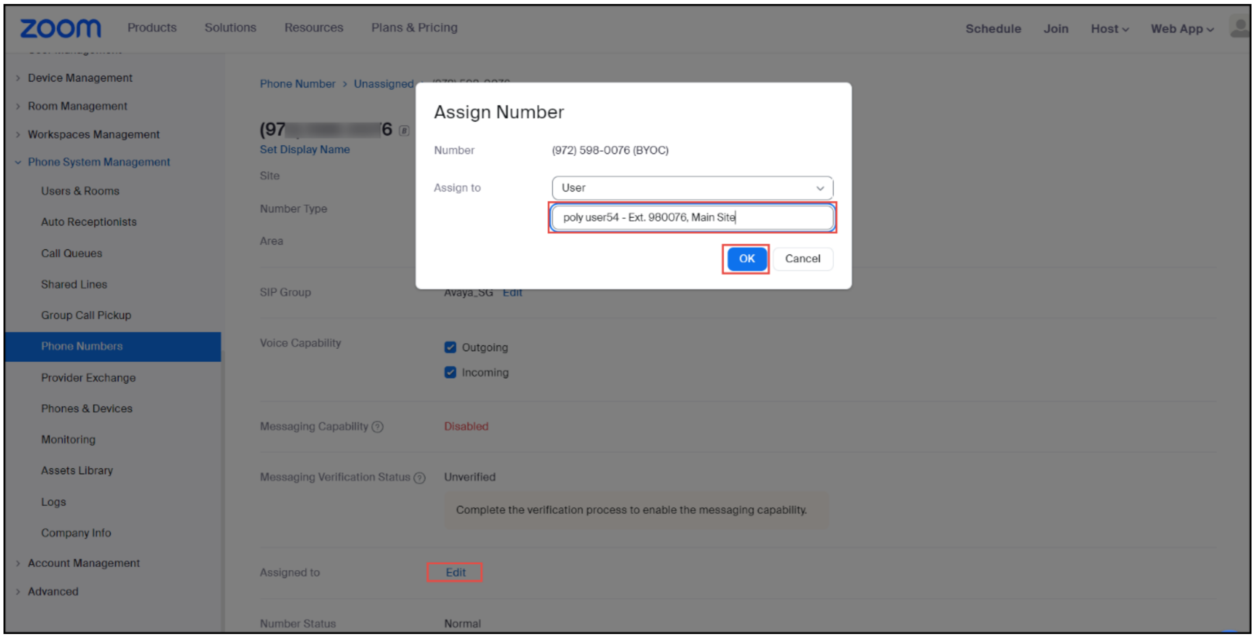
□	Number	Area	Number Type	Voice Capability	Messaging Capability	Messaging Verification Status	Number Status	Site
□	(4[redacted] B	United States	Toll Number	Incoming & Outgoing	Disabled	Unverified	Normal	Main Site

- Select the phone number that needs to be assigned to Zoom phone users



□	(9[redacted] B	United States	Toll Number	Incoming & Outgoing	Disabled	Unverified	Normal	Main Site
□	(97[redacted]6 B	United States	Toll Number	Incoming & Outgoing	Disabled	Unverified	Normal	Main Site
□	(9[redacted] B	United States	Toll Number	Incoming & Outgoing	Disabled	Unverified	Normal	Main Site

- Click on **Edit** near “**Assigned to**” as shown below in the screenshot
- A dialog box pops out and in **Assign to**: select the user you need to assign the phone number and click **OK**. The number will be assigned to the selected user



(97[redacted]6

Assign Number

Number (972) 598-0076 (BYOC)

Assign to User

poly user54 - Ext. 980076, Main Site

Site

Number Type

Area

SIP Group Avaya_SG Edit

Voice Capability ☑ Outgoing ☑ Incoming

Messaging Capability Disabled

Messaging Verification Status Unverified

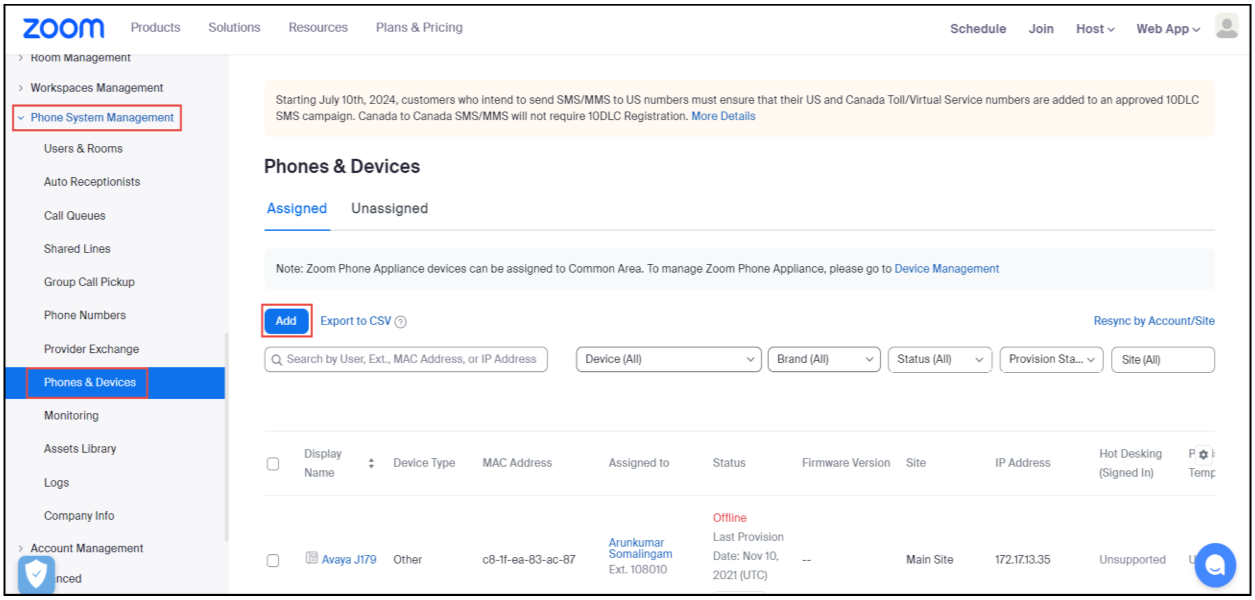
Complete the verification process to enable the messaging capability.

Assigned to Edit

Number Status Normal

3.7 Provisioning Phones for Zoom Phone Users

- Provision desk phones for Zoom Phone users. Zoom certified vendor phone models are used for this test and will be available as shown below after provisioning
- Navigate to **Phone System Management -> Phones & Devices ->Add**



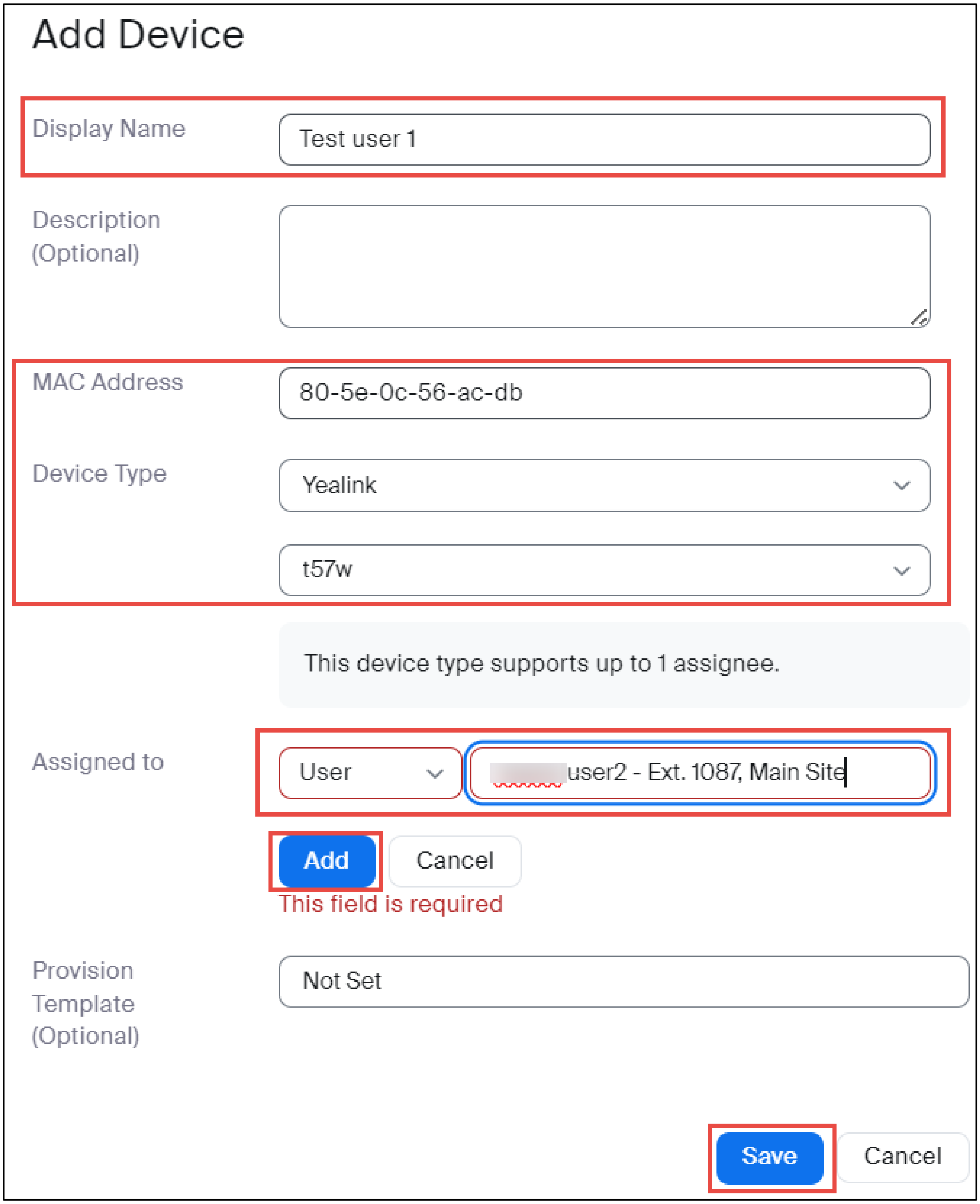
Starting July 10th, 2024, customers who intend to send SMS/MMS to US numbers must ensure that their US and Canada Toll/Virtual Service numbers are added to an approved 10DLC SMS campaign. Canada to Canada SMS/MMS will not require 10DLC Registration. More Details

Phones & Devices

Note: Zoom Phone Appliance devices can be assigned to Common Area. To manage Zoom Phone Appliance, please go to Device Management

□	Display Name	Device Type	MAC Address	Assigned to	Status	Firmware Version	Site	IP Address	Hot Desking (Signed In)	P Temp
□	Avaya J179	Other	c8-1f-ea-83-ac-87	Arunkumar Somalingam Ext. 108010	Offline Last Provision Date: Nov 10, 2021 (UTC)	--	Main Site	172.17.13.35	Unsupported	U

- **Display Name**: Provide the display name for the phone
- **MAC Address**: Enter the MAC Address of the Phone
- **Device Type**: Here Yealink t57w is used as an example
- **Assigned to**: Select the **user** to be assigned to the Phone and Click **Add**
- Click **Save**



Add Device

Display Name: Test user 1

Description (Optional):

MAC Address: 80-5e-0c-56-ac-db

Device Type: Yealink

t57w

This device type supports up to 1 assignee.

Assigned to: User [redacted]user2 - Ext. 1087, Main Site

This field is required

Provision Template (Optional): Not Set

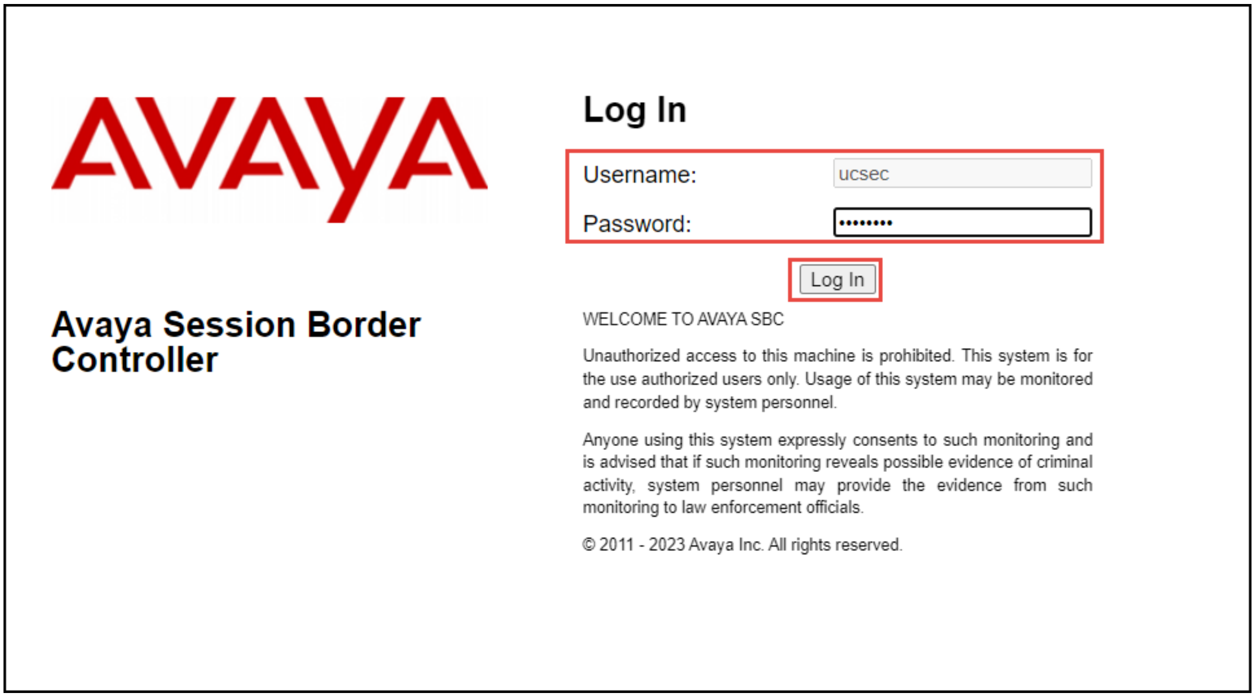
4 Configuration Steps-Avaya SBC

The Avaya Session Border Controller (SBC) is a critical component in modern enterprise communication networks, providing robust security and seamless interoperability for SIP-based Unified Communications (UC). Designed to terminate SIP trunks efficiently, the Avaya SBC offers a cost-effective solution without the complexity typically associated with traditional SBCs. One of the standout features of the Avaya SBC is its comprehensive security capabilities. It protects enterprise networks from various threats, including Denial of Service (DoS) attacks, toll fraud, and malformed packets. Additionally, it ensures privacy by hiding internal network topology and encrypting SIP signaling and media packets. Interoperability is another key strength of the Avaya SBC. It facilitates communication between different networks through Network Address Translation (NAT) and header manipulation within SIP messages. This ensures that diverse systems can work together smoothly. The Avaya SBC also supports regulatory compliance by prioritizing emergency calls and enabling lawful interception of communications. Its media services include interpreting DTMF tones, transcoding media, and supporting diverse media streams such as video.

This document outlines the configuration best practices for the Avaya SBC when deployed with Zoom Bring Your Own Carrier (BYOC). This means that for all subscribers catering to Zoom customers, the PSTN calls terminating through the SBC are directly connected to the Service Provider of their choice.

4.1 Avaya SBC Login

- Log into Avaya Session Border Controller for Enterprise (ASBCE) web interface by typing **“https://X.X.X.X/sbc”**
- Enter the **Username** and **Password and** Click **Log In**



Log In

Username: ucsec

Password: ••••••••

Log In

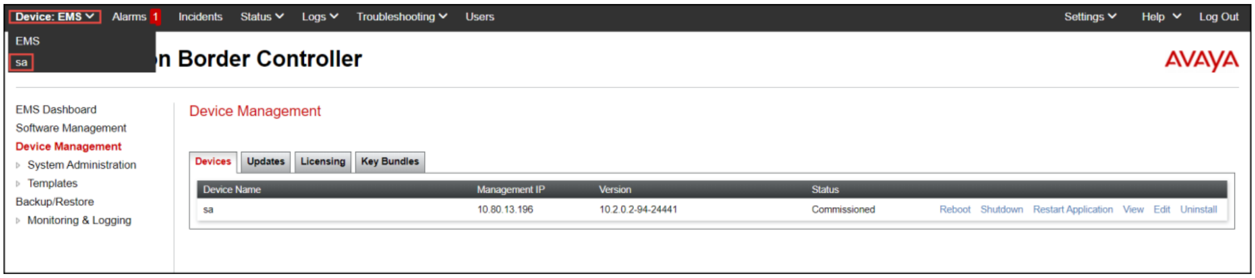
WELCOME TO AVAYA SBC

Unauthorized access to this machine is prohibited. This system is for the use authorized users only. Usage of this system may be monitored and recorded by system personnel.

Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence from such monitoring to law enforcement officials.

© 2011 - 2023 Avaya Inc. All rights reserved.

- Navigate to **Device: EMS** and select **sa** from drop down to expand the configuration for Avaya SBC



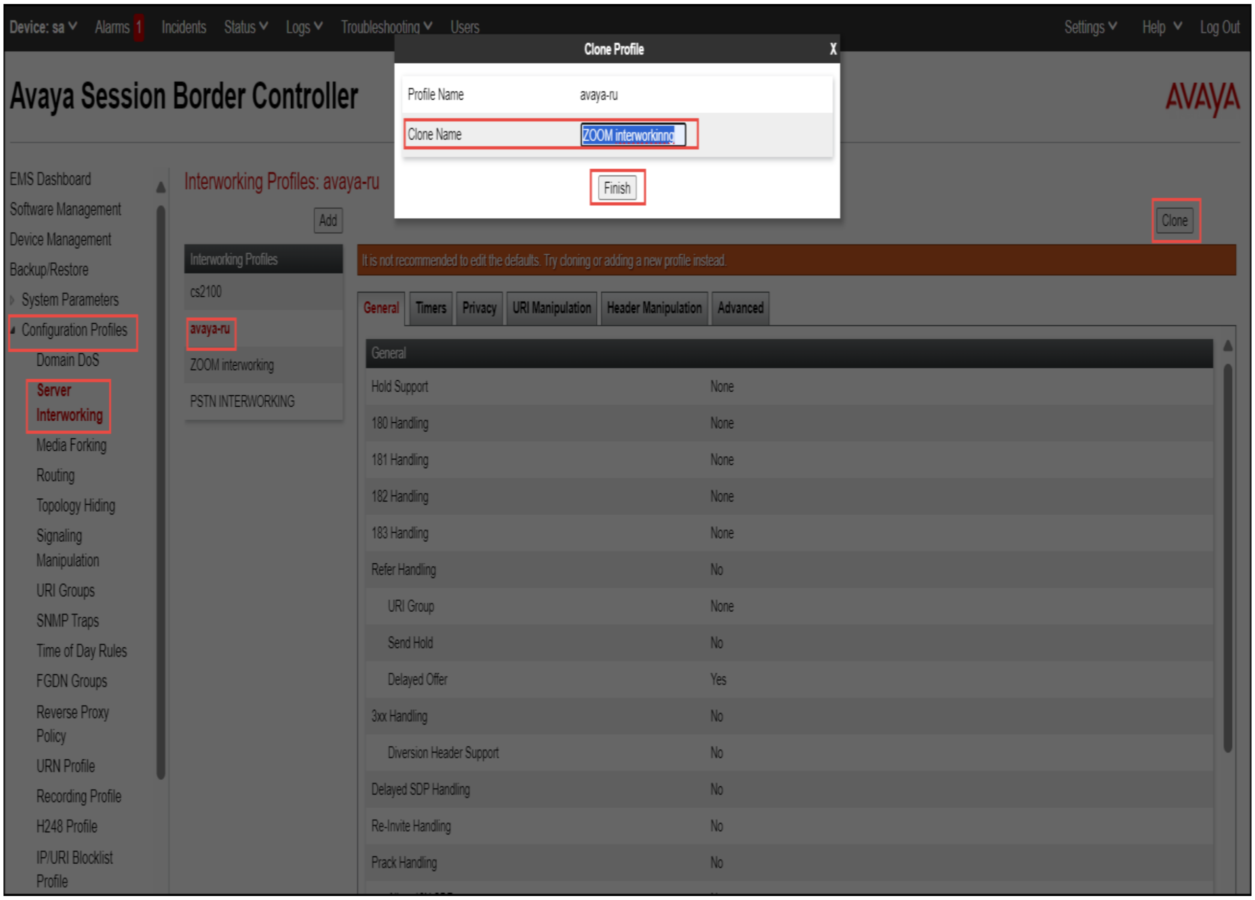
Device Management

Device Name	Management IP	Version	Status	
sa	10.80.13.196	10.2.0.2-94-24441	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

4.2 Zoom Leg Configuration

4.2.1 Server Interworking for Zoom PBX

- Navigate to **Configuration Profiles > Server Interworking**
- Select the default Interworking Profile **avaya-ru**, click **Clone**
- Set Clone Name: **ZOOM interworking**
- Click **Finish**



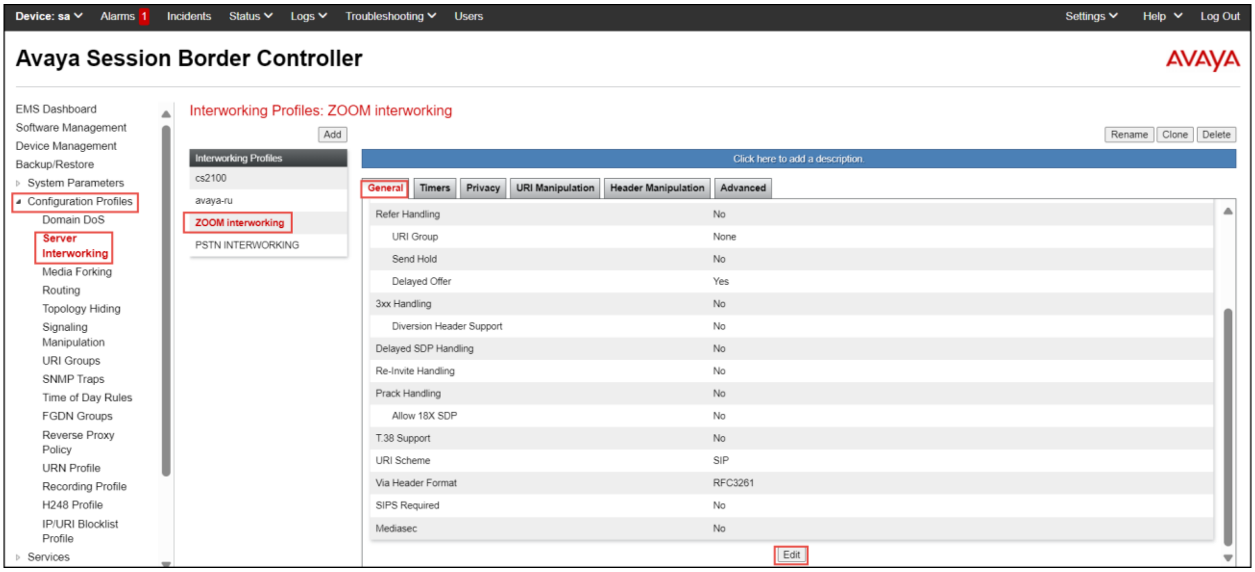
Profile Name avaya-ru

Clone Name ZOOM interworking

It is not recommended to edit the defaults. Try cloning or adding a new profile instead.

General	
Hold Support	None
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	Yes
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No

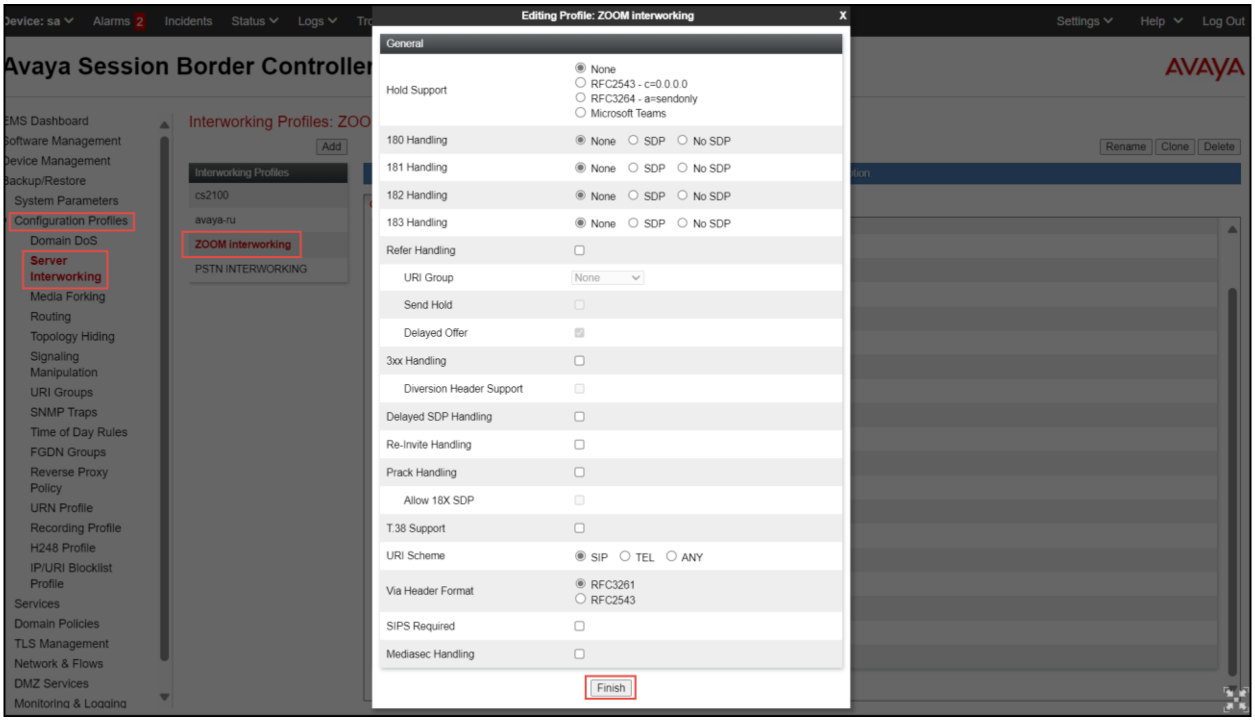
- Select **Zoom Interworking** that we had created in above step
- Select **General** tab and click **Edit**



Interworking Profiles: ZOOM interworking

Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	Yes
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261
SIPS Required	No
Mediasec	No

- All parameters are set to default, refer the below figure
- Click on **Finish**

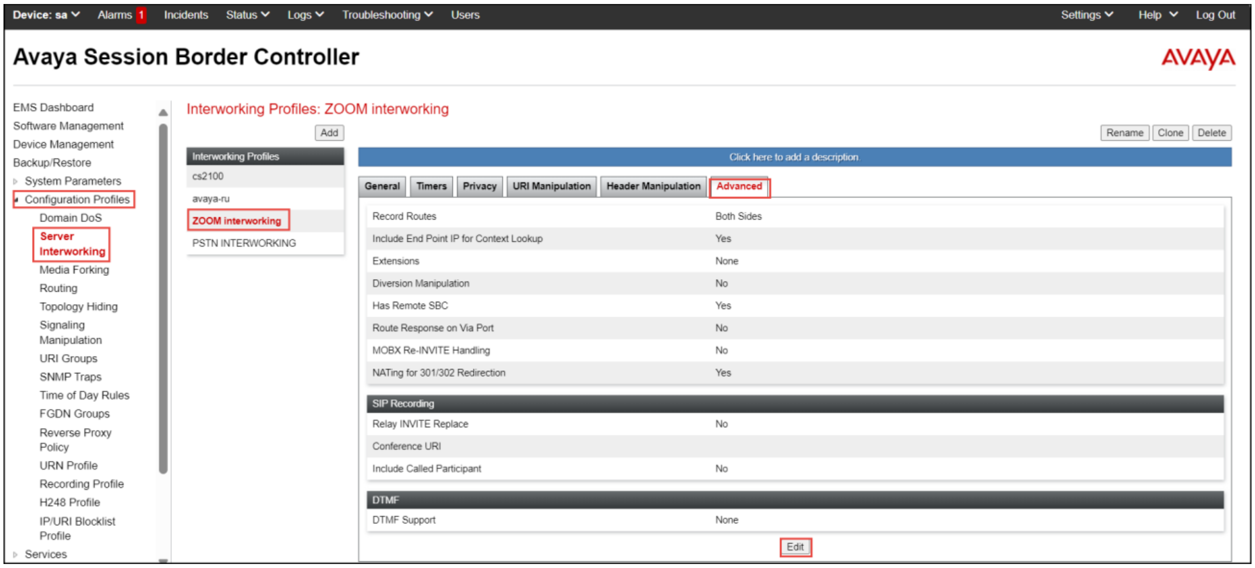


Editing Profile: ZOOM interworking

General

Hold Support	● None ○ RFC2543 - c=0.0.0.0 ○ RFC3264 - a=sendonly ○ Microsoft Teams
180 Handling	● None ○ SDP ○ No SDP
181 Handling	● None ○ SDP ○ No SDP
182 Handling	● None ○ SDP ○ No SDP
183 Handling	● None ○ SDP ○ No SDP
Refer Handling	□
URI Group	None
Send Hold	□
Delayed Offer	☑
3xx Handling	□
Diversion Header Support	□
Delayed SDP Handling	□
Re-Invite Handling	□
Prack Handling	□
Allow 18X SDP	□
T.38 Support	□
URI Scheme	● SIP ○ TEL ○ ANY
Via Header Format	● RFC3261 ○ RFC2543
SIPS Required	□
Mediasec Handling	□

- Select **Advanced** tab and click **Edit**

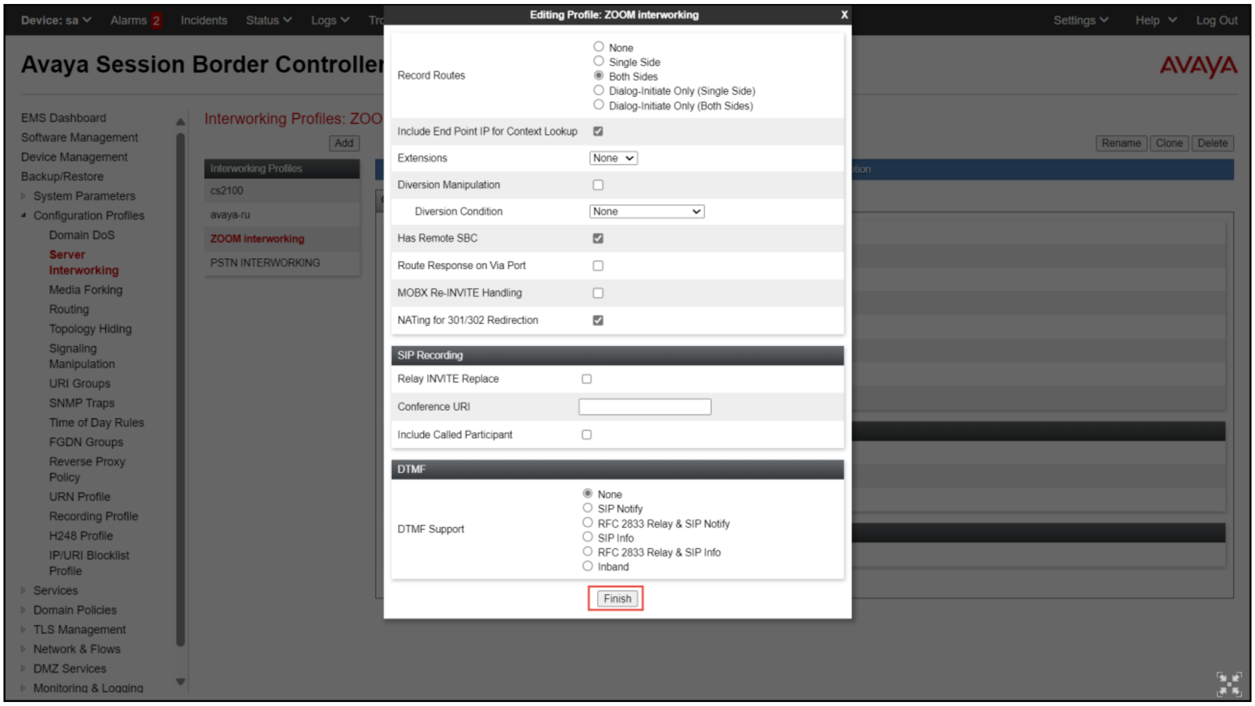


Avaya Session Border Controller

Interworking Profiles: ZOOM interworking

Record Routes	Both Sides
Include End Point IP for Context Lookup	Yes
Extensions	None
Diversion Manipulation	No
Has Remote SBC	Yes
Route Response on Via Port	No
MOBX Re-INVITE Handling	No
NATing for 301/302 Redirection	Yes
SIP Recording	
Relay INVITE Replace	No
Conference URI	
Include Called Participant	No
DTMF	
DTMF Support	None

- All parameters are set to default, refer the below figure
- Click on **Finish**

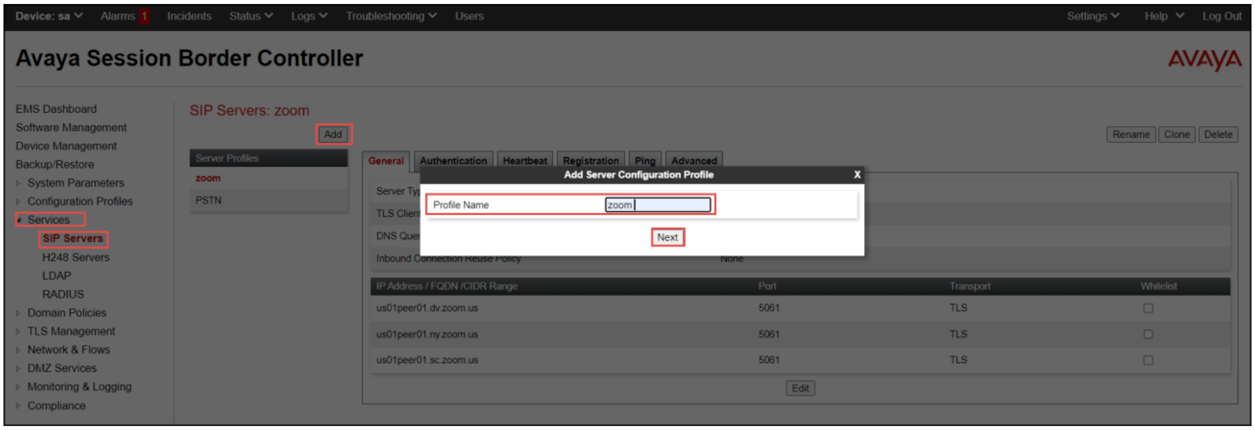


Editing Profile: ZOOM interworking

Record Routes	○ None ○ Single Side ● Both Sides ○ Dialog-Initiate Only (Single Side) ○ Dialog-Initiate Only (Both Sides)
Include End Point IP for Context Lookup	☑
Extensions	None
Diversion Manipulation	□
Diversion Condition	None
Has Remote SBC	☑
Route Response on Via Port	□
MOBX Re-INVITE Handling	□
NATing for 301/302 Redirection	☑
SIP Recording	
Relay INVITE Replace	□
Conference URI	
Include Called Participant	□
DTMF	
DTMF Support	● None ○ SIP Notify ○ RFC 2833 Relay & SIP Notify ○ SIP Info ○ RFC 2833 Relay & SIP Info ○ Inband

4.2.2 SIP Server

- Navigate to **Services > SIP Servers**
- Click **Add**
- Set Profile Name: **zoom**
- Click **Next**



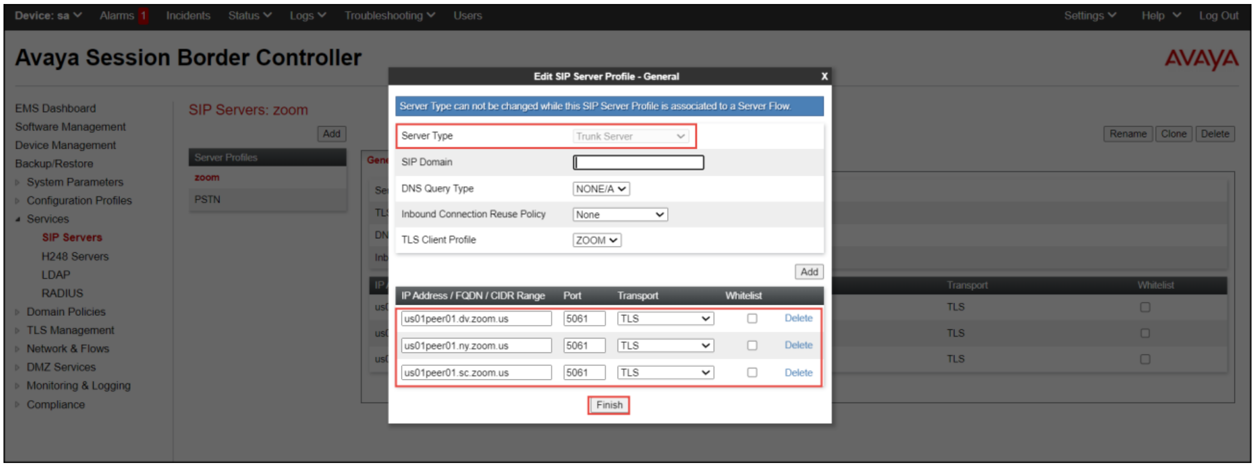
SIP Servers: zoom

Add Server Configuration Profile

Profile Name	zoom

IP Address / FQDN /CIDR Range	Port	Transport	Whitelist
us01peer01.dv.zoom.us	5061	TLS	□
us01peer01.ny.zoom.us	5061	TLS	□
us01peer01.sc.zoom.us	5061	TLS	□

- Set Server Type: Select **Trunk Server** from the drop down
- Set IP Address/FQDN/CIDR Range: Enter the **Zoom PBX FQDNs**
- Set Port: **5061**
- Set Transport: **TLS**
- Click **Finish**



SIP Servers: zoom

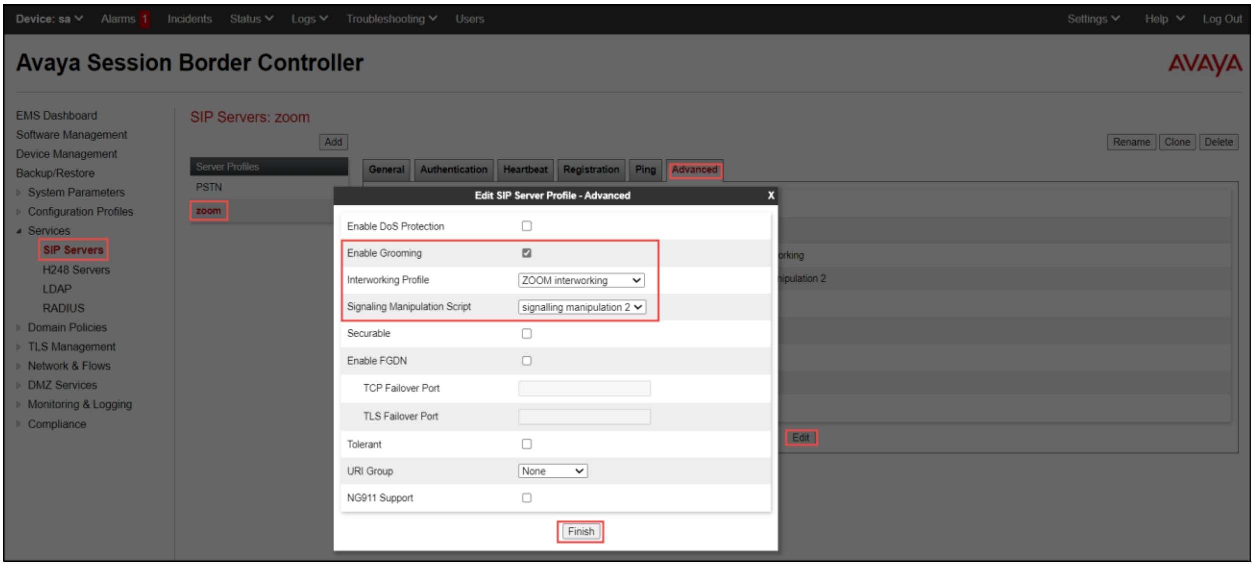
Edit SIP Server Profile - General

Server Type can not be changed while this SIP Server Profile is associated to a Server Flow.

Server Type	Trunk Server
SIP Domain	
DNS Query Type	NONE/A
Inbound Connection Reuse Policy	None
TLS Client Profile	ZOOM

IP Address / FQDN / CIDR Range	Port	Transport	Whitelist	
us01peer01.dv.zoom.us	5061	TLS	□	Delete
us01peer01.ny.zoom.us	5061	TLS	□	Delete
us01peer01.sc.zoom.us	5061	TLS	□	Delete

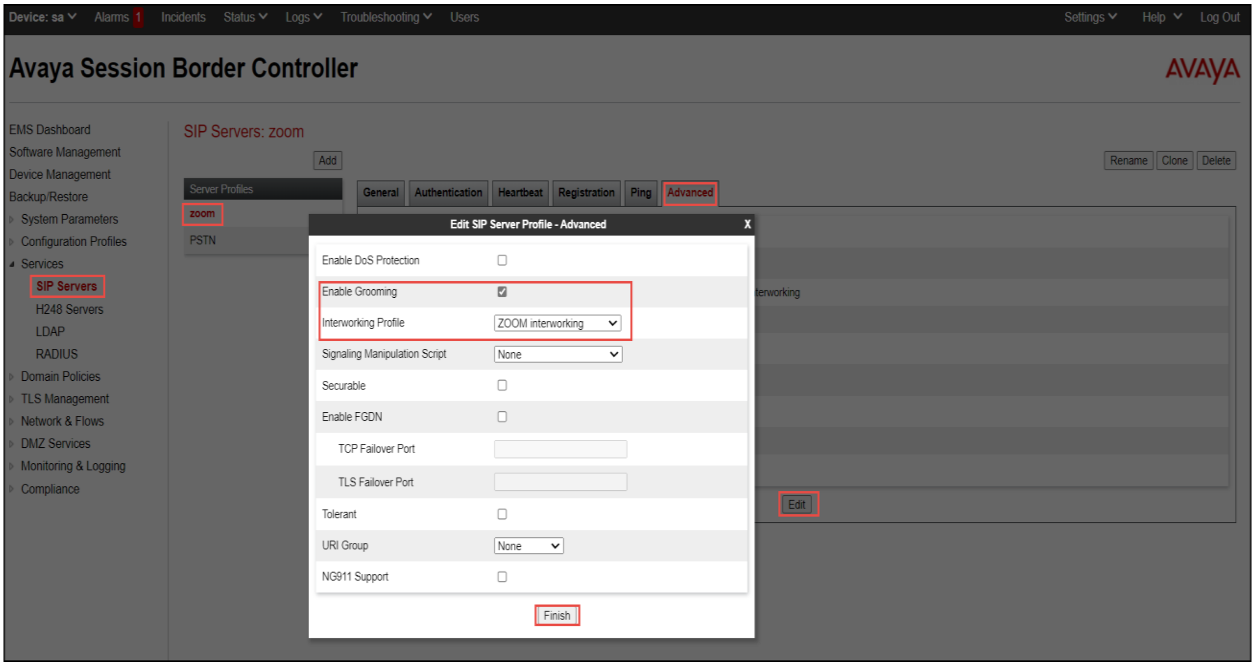
- Navigate to **SIP Servers > zoom > Advanced** tab
- Click **Edit**
- Enable Grooming: **Checked**
- Signaling Manipulation Script: **signaling manipulation 2** (Refer 4.2.12.2 FQDN to IP Manipulation)
- Interworking Profile: Select **ZOOM interworking**
- Click on **Finish**



Edit SIP Server Profile - Advanced

Enable DoS Protection	□
Enable Grooming	☑
Interworking Profile	ZOOM interworking
Signaling Manipulation Script	signalling manipulation 2
Securable	□
Enable FGDN	□
TCP Failover Port	
TLS Failover Port	
Tolerant	□
URI Group	None
NG911 Support	□

Finish



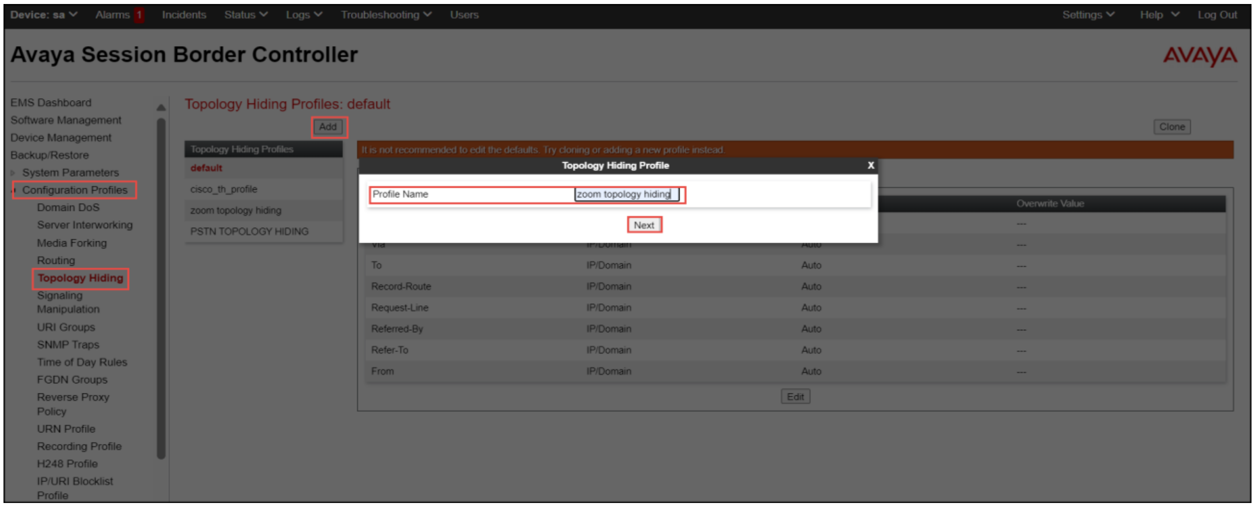
Edit SIP Server Profile - Advanced

Enable DoS Protection	□
Enable Grooming	☑
Interworking Profile	ZOOM interworking
Signaling Manipulation Script	None
Securable	□
Enable FGDN	□
TCP Failover Port	
TLS Failover Port	
Tolerant	□
URI Group	None
NG911 Support	□

Finish

4.2.3Topology Hiding

- Navigate: **Configuration Profiles** > **Topology Hiding**
- Click **Add**
- Set Profile Name: **zoom topology hiding**
- Click **Next**



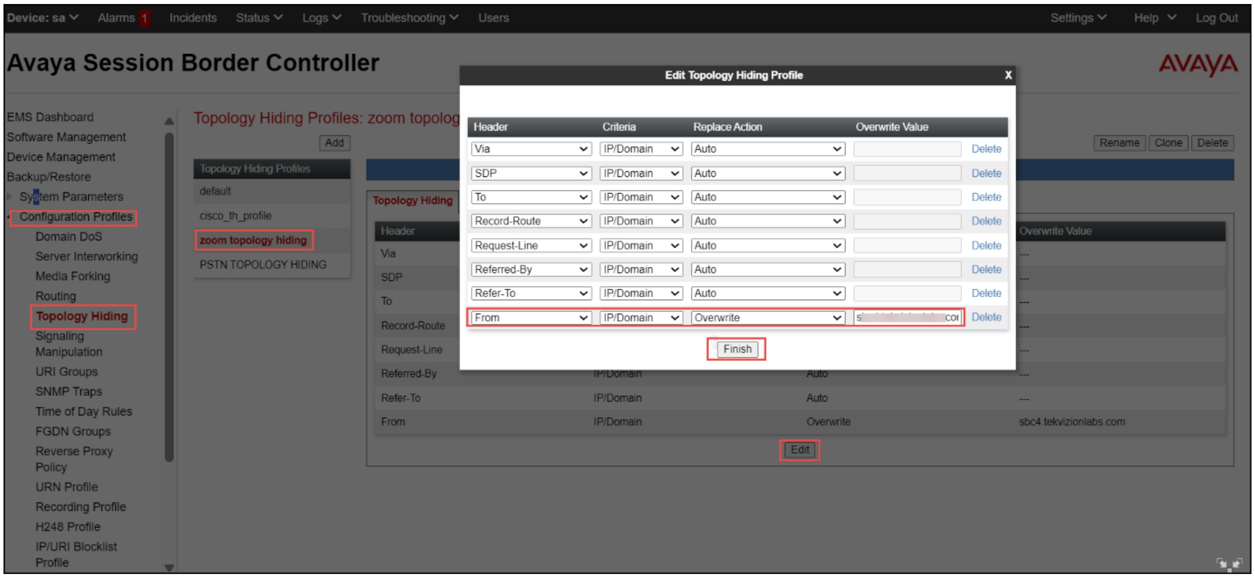
It is not recommended to edit the defaults. Try cloning or adding a new profile instead.

Profile Name: zoom topology hiding

			Overwrite Value

Via	IP/Domain	Auto	---
To	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
Request-Line	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
From	IP/Domain	Auto	---

- Select the newly created profile **zoom topology hiding** and click **Edit**
- **Overwrite Value**: Replace the **From header** with ZOOM PBX Facing Public FQDN
- Click **Finish**



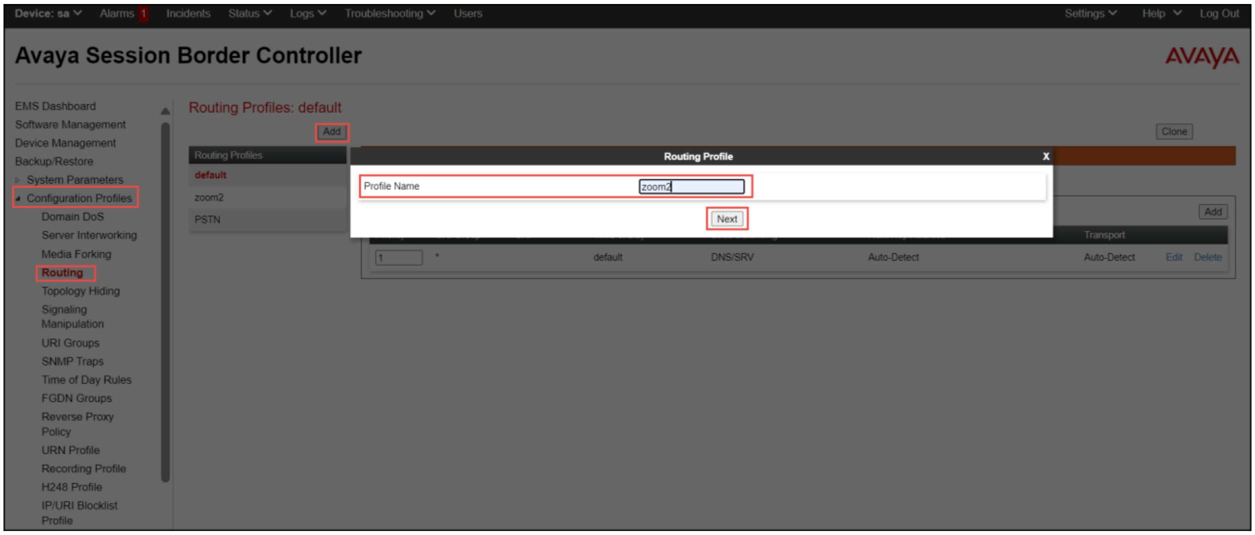
Edit Topology Hiding Profile

Header	Criteria	Replace Action	Overwrite Value	
Via	IP/Domain	Auto		Delete
SDP	IP/Domain	Auto		Delete
To	IP/Domain	Auto		Delete
Record-Route	IP/Domain	Auto		Delete
Request-Line	IP/Domain	Auto		Delete
Referred-By	IP/Domain	Auto		Delete
Refer-To	IP/Domain	Auto		Delete
From	IP/Domain	Overwrite	s[redacted]col	Delete

Header	Criteria	Replace Action	Overwrite Value
Via			---
SDP			---
To			---
Record-Route			---
Request-Line			---
Referred-By	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
From	IP/Domain	Overwrite	sbc4.tekvizionlabs.com

4.2.4 Routing

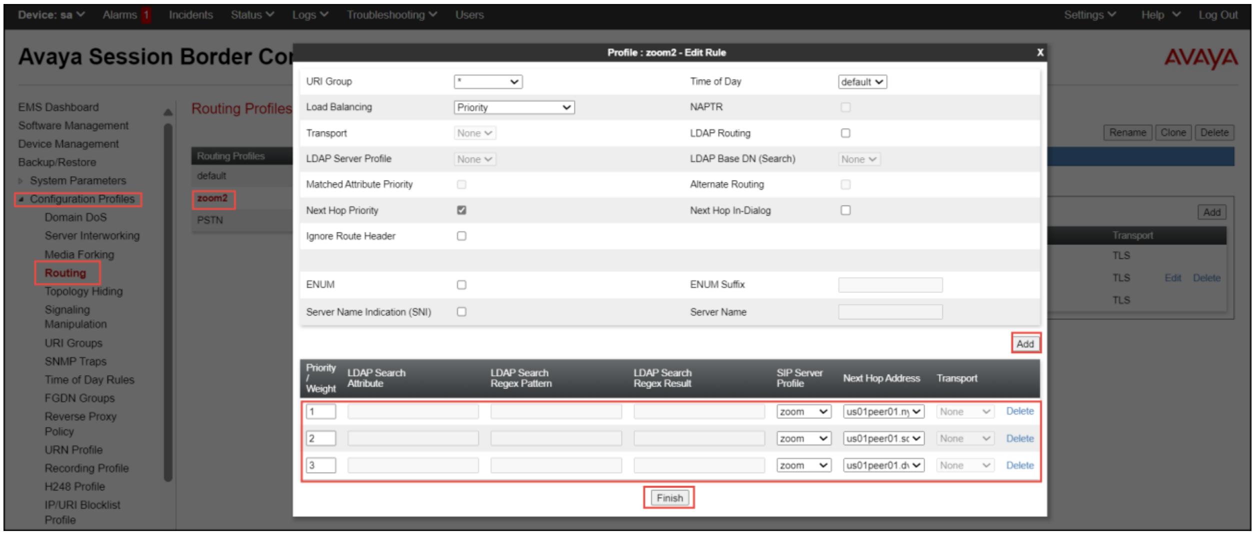
- Navigate to **Configuration Profiles > Routing**
- Click **Add**
- Set Profile Name: **zoom2**
- Click **Next**



Profile Name: zoom2

1	*	default	DNS/SRV	Auto-Detect	Auto-Detect	Edit Delete

- At **Routing Profile** Window, Click **Add.**
- Set Priority/Weight: **1, 2, 3.**
- Select SIP Server Profile: **zoom** from the drop-down menu.
- Select Next Hop Address: Zoom PBX FQDN according to priority.
- Click **Finish.**



Profile : zoom2 - Edit Rule

URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	□
Transport	None	LDAP Routing	□
LDAP Server Profile	None	LDAP Base DN (Search)	None
Matched Attribute Priority	□	Alternate Routing	□
Next Hop Priority	☑	Next Hop In-Dialog	□
Ignore Route Header	□		
ENUM	□	ENUM Suffix	
Server Name Indication (SNI)	□	Server Name	

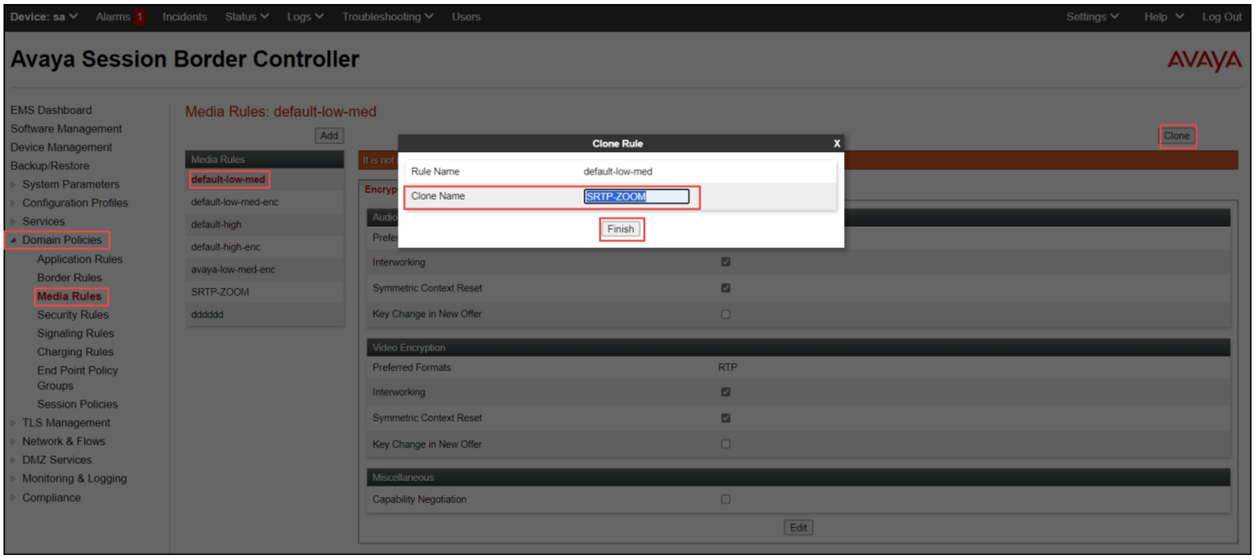
Add

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport	
1				zoom	us01peer01.n	None	Delete
2				zoom	us01peer01.sc	None	Delete
3				zoom	us01peer01.d	None	Delete

Finish

4.2.5 Media Rules

- Navigate to **Domain Policies > Media Rules**
- Select Media Rules **default-low-med** Click Clone
- Set **Clone Name: SRTP-ZOOM**
- Click on **Finish**



Media Rules: default-low-med

Clone Rule

Rule Name	default-low-med
Clone Name	SRTP-ZOOM

Finish

Interworking	☑
Symmetric Context Reset	☑
Key Change in New Offer	□

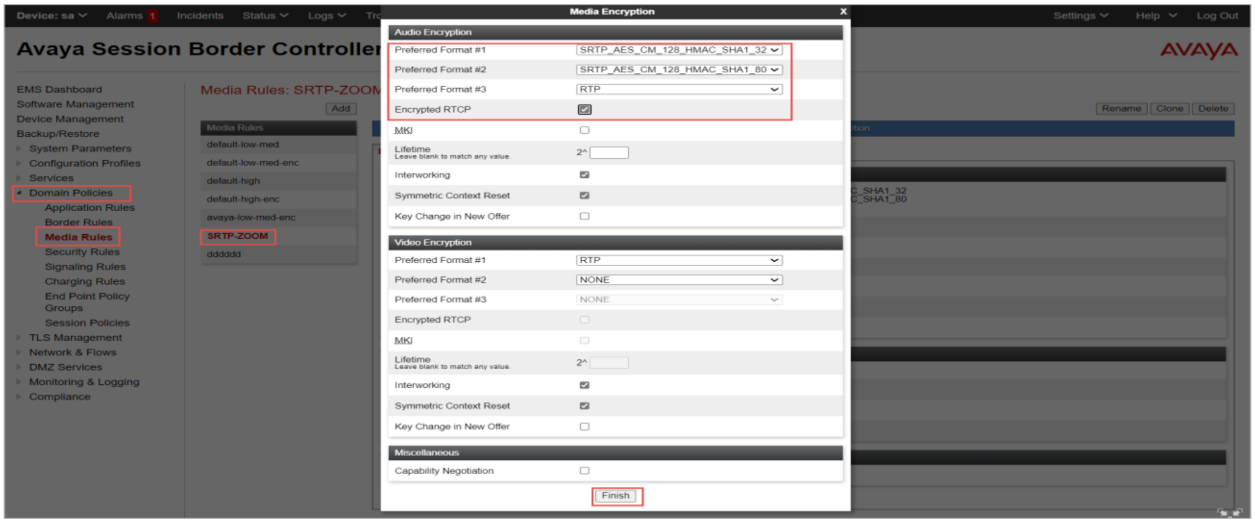
Video Encryption

Preferred Formats	RTP
Interworking	☑
Symmetric Context Reset	☑
Key Change in New Offer	□

Miscellaneous

Capability Negotiation	□

- Select newly created Media Rules **SRTP-ZOOM**
- Set Preferred Formats: **SRTP_AES_CM_128_HMAC_SHA1_32, SRTP_AES_CM_128_HMAC_SHA1_80, RTP**
- Set Encrypted RTCP: **Checked**
- Click on **Finish.**



Media Encryption

Audio Encryption

Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_32
Preferred Format #2	SRTP_AES_CM_128_HMAC_SHA1_80
Preferred Format #3	RTP
Encrypted RTCP	☑
MKI	☐
Lifetime Leave blank to match any value.	2^
Interworking	☑
Symmetric Context Reset	☑
Key Change in New Offer	☐

Video Encryption

Preferred Format #1	RTP
Preferred Format #2	NONE
Preferred Format #3	NONE
Encrypted RTCP	☐
MKI	☐
Lifetime Leave blank to match any value.	2^
Interworking	☑
Symmetric Context Reset	☑
Key Change in New Offer	☐

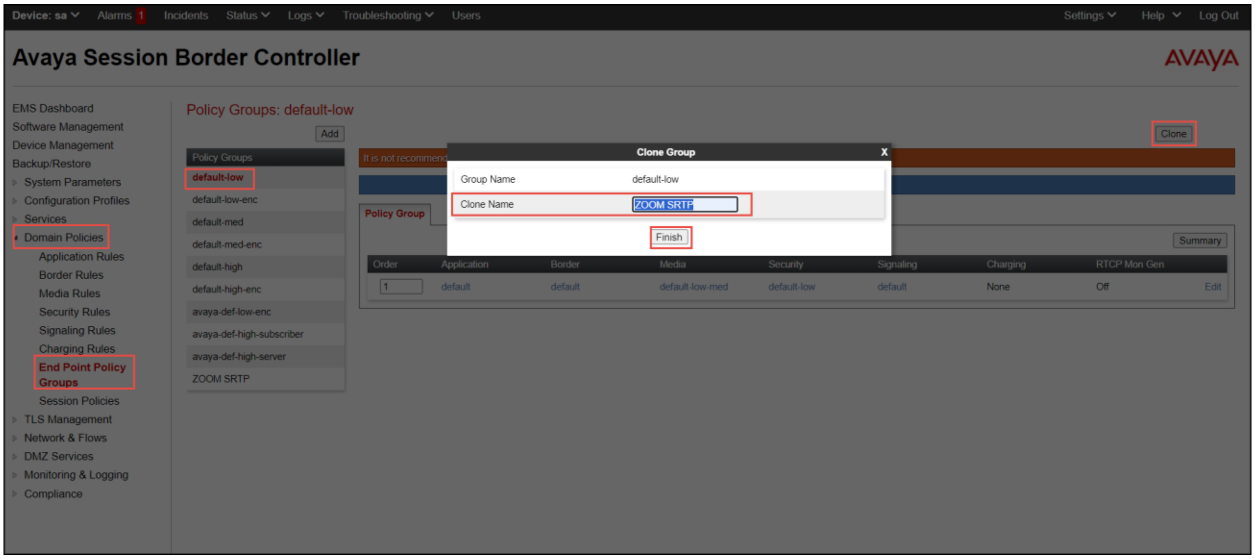
Miscellaneous

Capability Negotiation	☐

Finish

4.2.6 End Point Policy Groups

- Navigate to **Domain Policies > End Point Policy Groups**
- Select **default-low** under Policy Groups
- Click **Clone**
- Set Clone Name: **ZOOM SRTP**
- Click **Finish.**



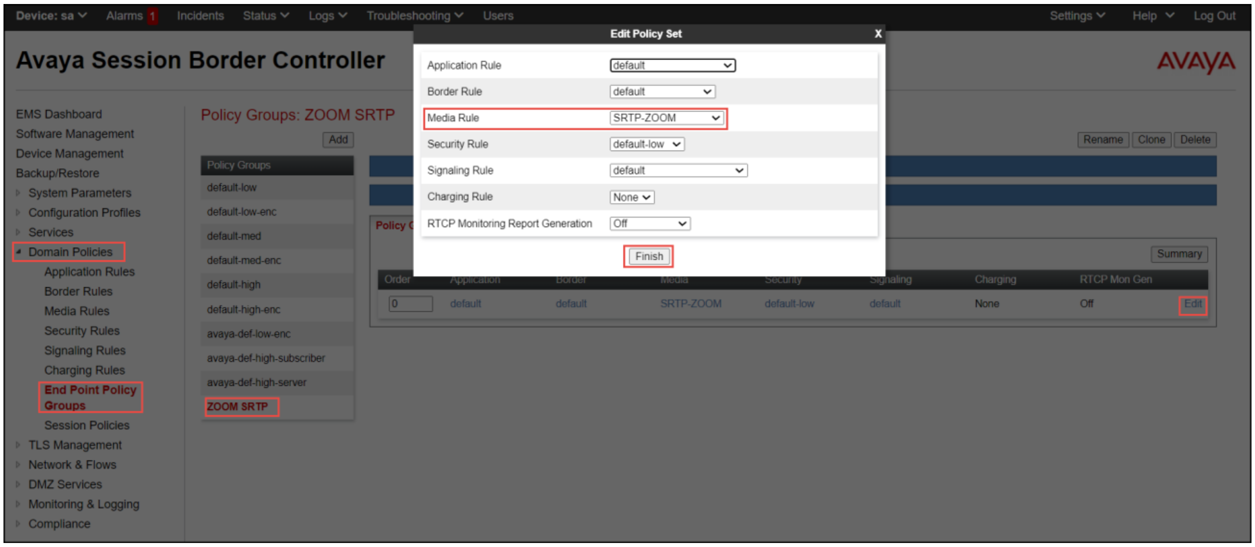
Clone Group

Group Name	default-low
Clone Name	ZOOM SRTP

Finish

Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen	
1	default	default	default-low-med	default-low	default	None	Off	Edit

- Select the newly created Group **ZOOM SRTP** and click **Edit**
- Set Media Rule: **SRTP-ZOOM**
- Click **Finish**



Edit Policy Set

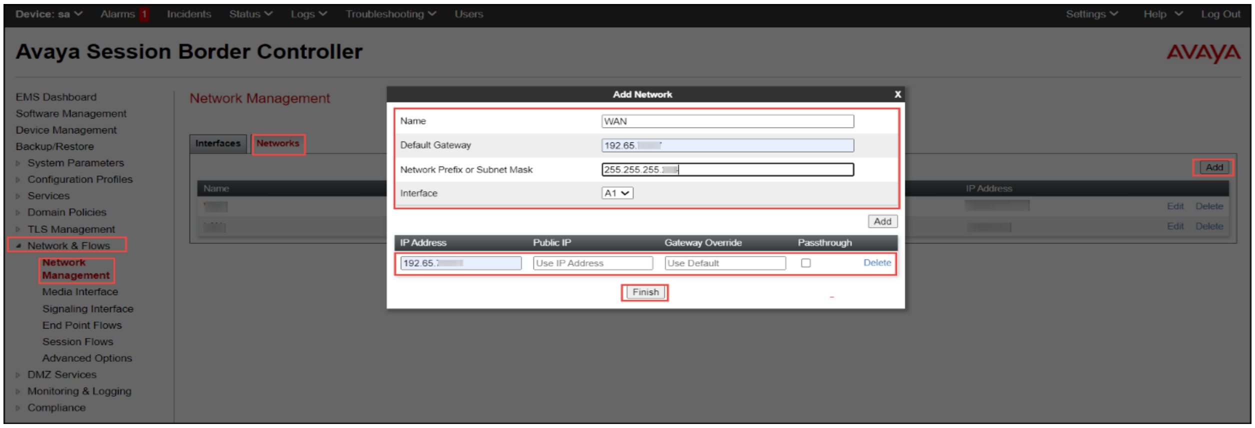
Application Rule	default
Border Rule	default
Media Rule	SRTP-ZOOM
Security Rule	default-low
Signaling Rule	default
Charging Rule	None
RTCP Monitoring Report Generation	Off

Finish

Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen	
0	default	default	SRTP-ZOOM	default-low	default	None	Off	Edit

4.2.7 Network Management

- Navigate to **Network & Flows > Network Management >Networks**
- Click **Add.** A window will appear titled **Add Network**
- Set Name: **WAN** is given for the network facing **ZOOM PBX**
- Set Default Gateway: **192.65.XX.XX**
- Set Network Prefix or Subnet Mask: **255.255.255.XXX**
- Set Interface: **A1**
- Set IP Address: **192.65.XX.XX** facing ZOOM PBX
- Click **Finish**



Add Network

Name	WAN
Default Gateway	192.65.[redacted]
Network Prefix or Subnet Mask	255.255.255.[redacted]
Interface	A1

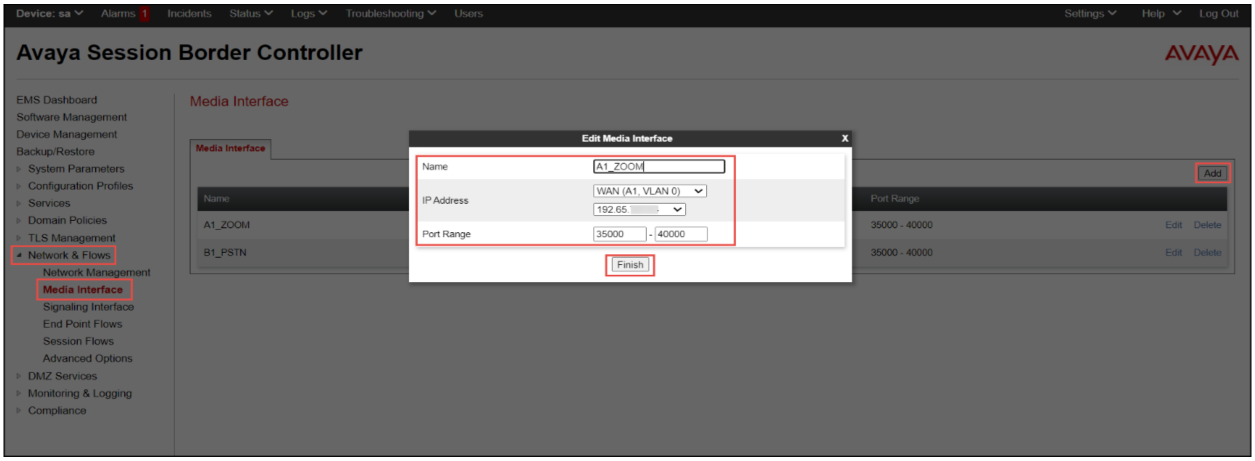
Add

IP Address	Public IP	Gateway Override	Passthrough	
192.65.[redacted]	Use IP Address	Use Default	□	Delete

Finish

4.2.8 Media Interface

- Navigate to **Network & Flows > Media Interface**. Click **Add**
- Set Name: **A1_ZOOM** is given here
- Set IP Address: Select WAN(A1,VLAN0) from the drop down and the IP address populates automatically. The IP address for Interface facing ZOOM PBX is **192.65.XX.XX**
- Set Port Range: **35000-40000**
- Click **Finish.**



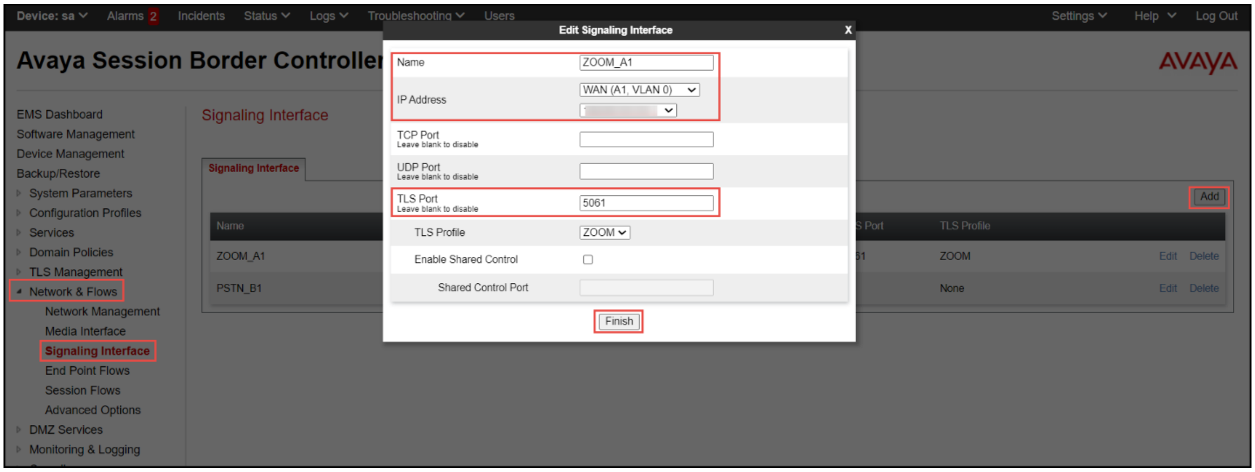
Edit Media Interface

Name	A1_ZOOM
IP Address	WAN (A1, VLAN 0) 192.65.[redacted]
Port Range	35000 - 40000

Name	Port Range		
A1_ZOOM	35000 - 40000	Edit	Delete
B1_PSTN	35000 - 40000	Edit	Delete

4.2.9 Signaling Interface

- Navigate to **Network & Flows > Signaling Interface**. Click **Add**, a new Add Signaling Interface window appears
- Set Name: **ZOOM_A1** is given for the interface facing **ZOOM PBX**
- Set IP Address: Select **WAN(A1,VLAN0)**
- Set TLS Port: **5061**
- Click **Finish**



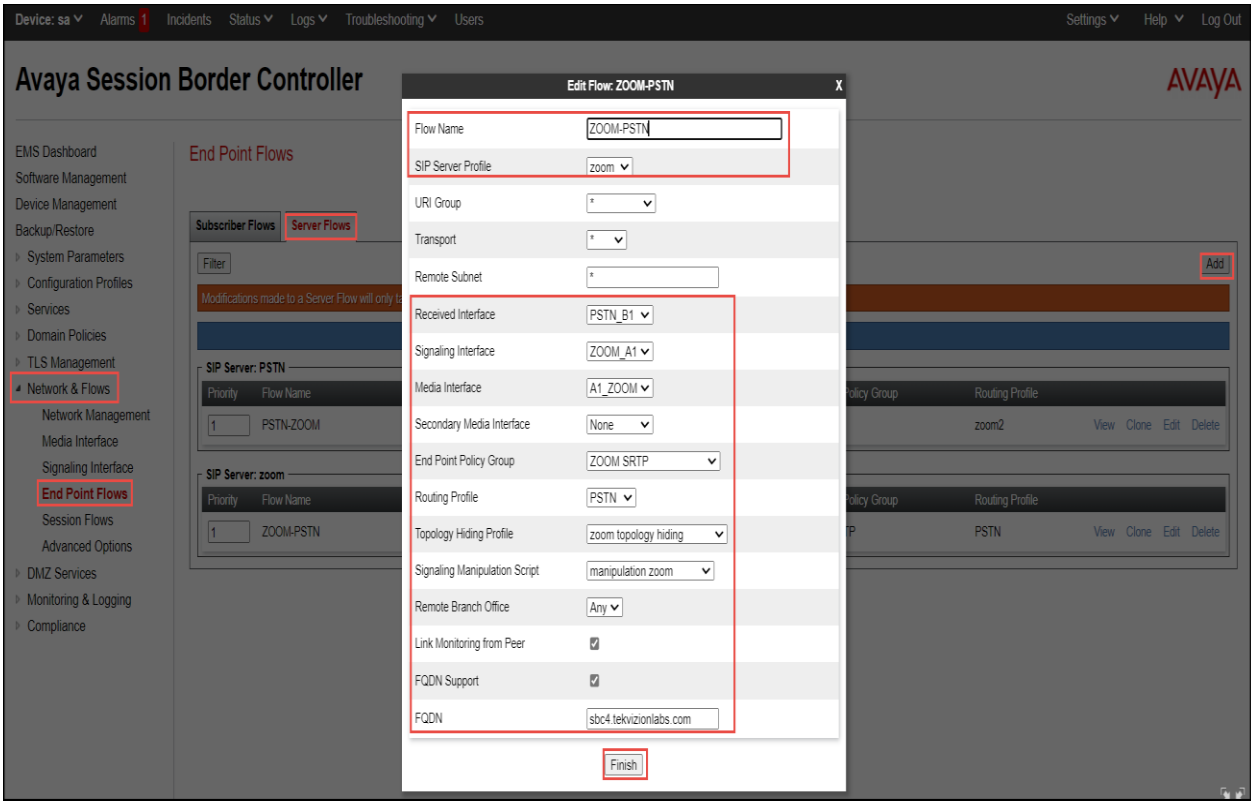
Edit Signaling Interface

Name	ZOOM_A1
IP Address	WAN (A1, VLAN 0) [redacted]
TCP Port Leave blank to disable	
UDP Port Leave blank to disable	
TLS Port Leave blank to disable	5061
TLS Profile	ZOOM
Enable Shared Control	□
Shared Control Port	

Name	S Port	TLS Profile		
ZOOM_A1	61	ZOOM	Edit	Delete
PSTN_B1		None	Edit	Delete

4.2.10 End Point Flow

- Navigate to **Network & Flows** > **End Point Flows** > **Server Flows** and Click **Add**
- Set Flow Name**: ZOOM-PSTN**
- Set SIP Server Profile: **zoom**
- Received Interface: **PSTN_B1**
- Signaling Interface**: ZOOM_A1**
- Media Interface: **A1_ZOOM**
- End Point Policy Group: **ZOOM SRTP**
- Routing Profile: **PSTN**
- Topology Hiding Profile**: zoom topology hiding**
- Signaling Manipulation Script**: manipulation zoom** (Refer 4.2.12.1 Signaling Manipulation)
- Link Monitoring from Peer: **Checked**
- FQDN Support**: Checked**
- FQDN: sbc4.tekvizionlabs.com
- Leave the other parameters set to default.
- Click on **Finish**



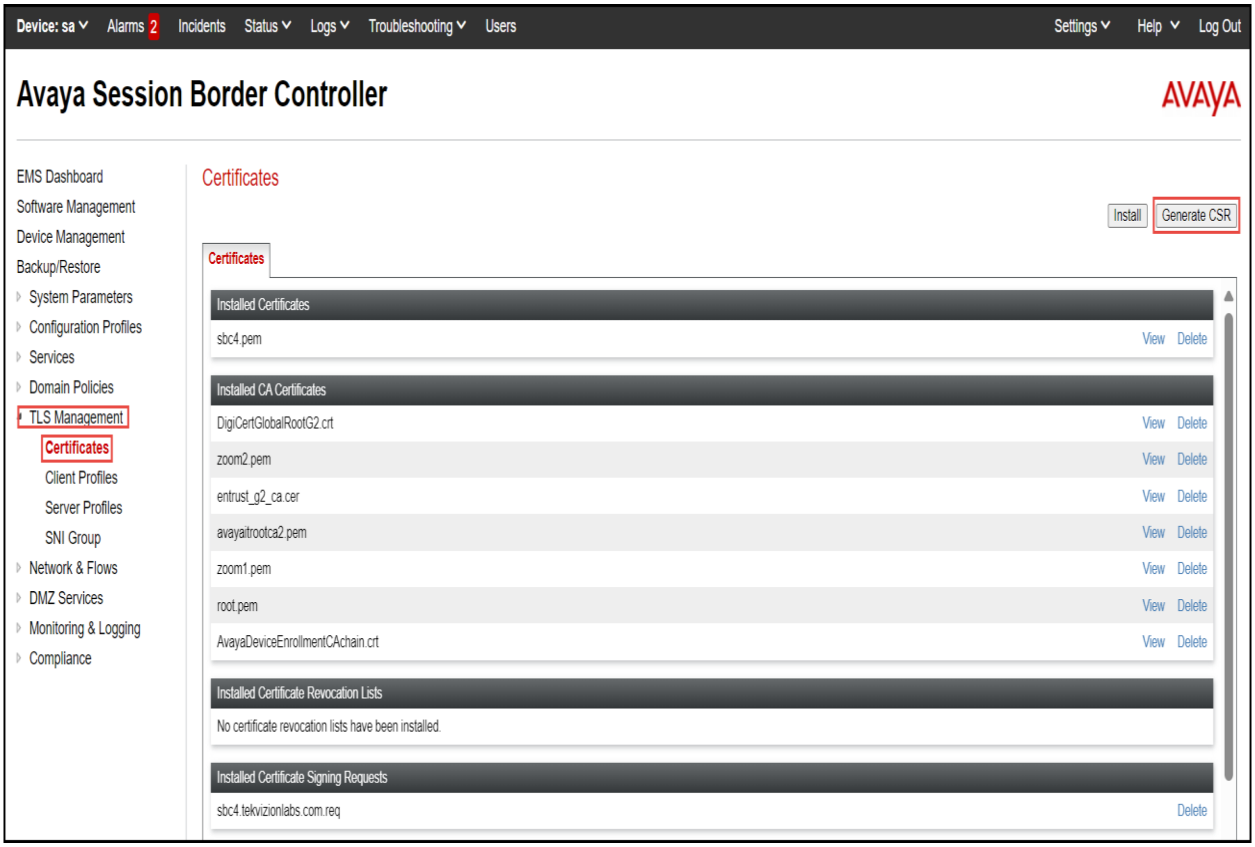
Edit Flow: ZOOM-PSTN

Flow Name	ZOOM-PSTN
SIP Server Profile	zoom
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	PSTN_B1
Signaling Interface	ZOOM_A1
Media Interface	A1_ZOOM
Secondary Media Interface	None
End Point Policy Group	ZOOM SRTP
Routing Profile	PSTN
Topology Hiding Profile	zoom topology hiding
Signaling Manipulation Script	manipulation zoom
Remote Branch Office	Any
Link Monitoring from Peer	☑
FQDN Support	☑
FQDN	sbc4.tekvizionlabs.com

4.2.11 TLS Profile

4.2.11.1 Generate CSR

- Navigate: **TLS management > Certificates**. Click **Generate CSR.**



Certificates

Installed Certificates

sbc4.pem View Delete

Installed CA Certificates

DigiCertGlobalRootG2.crt View Delete

zoom2.pem View Delete

entrust_g2_ca.cer View Delete

avayaitrootca2.pem View Delete

zoom1.pem View Delete

root.pem View Delete

AvayaDeviceEnrollmentCAchain.crt View Delete

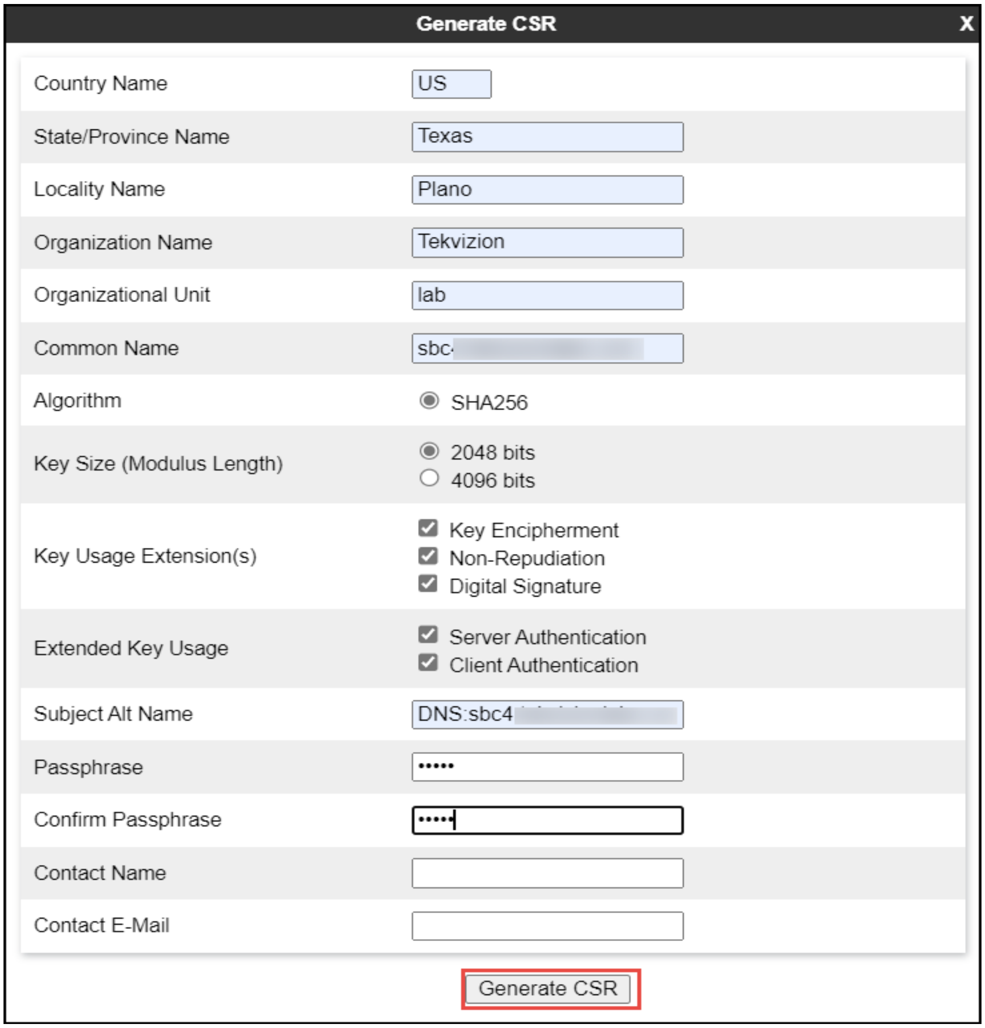
Installed Certificate Revocation Lists

No certificate revocation lists have been installed.

Installed Certificate Signing Requests

sbc4.tekvizionlabs.com.req Delete

- Set Country Name: **US**
- State/Province Name**: Texas**
- Locality Name**: Plano**
- Organization Name**: Tekvizion**
- Organizational Unit**: lab**
- Common Name**: sbc4.tekvizionlabs.com**
- Select Algorithm**: SHA256**
- Select Key Size (Modulus Length): 2048 bits
- In Key Usage Extension(s): Key Encipherment, Non-Repudiation, Digital Signature is **checked**
- In Extended Key Usage: Server Authentication, Client Authentication is **checked**
- Subject Alt Name**: DNS: sbc4tekvizionlabs.com**
- Set Passphrase & Confirm Passphrase**: XXXXX**
- Click **Generate CSR**

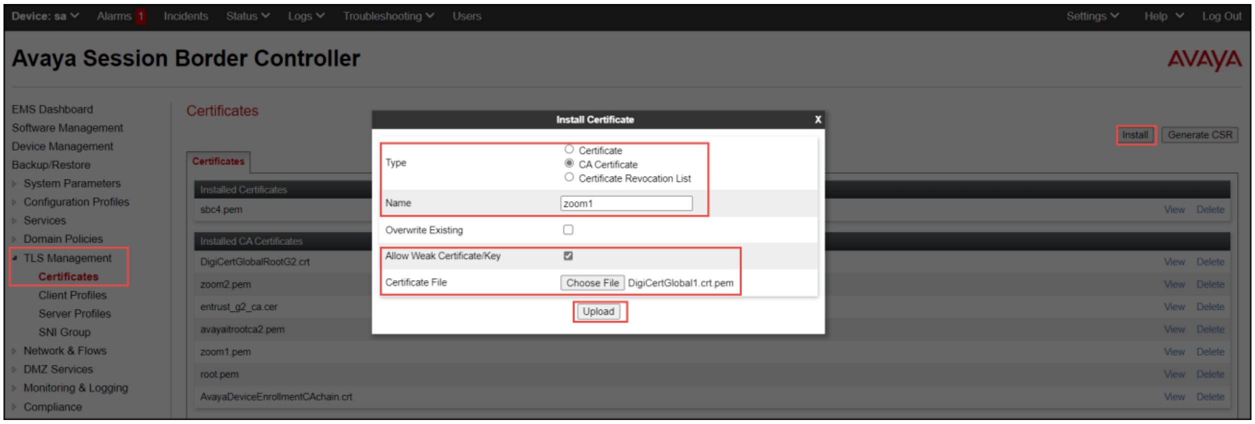


Generate CSR

Country Name	US
State/Province Name	Texas
Locality Name	Plano
Organization Name	Tekvizion
Organizational Unit	lab
Common Name	sbc[redacted]
Algorithm	● SHA256
Key Size (Modulus Length)	● 2048 bits ○ 4096 bits
Key Usage Extension(s)	☑ Key Encipherment ☑ Non-Repudiation ☑ Digital Signature
Extended Key Usage	☑ Server Authentication ☑ Client Authentication
Subject Alt Name	DNS:sbc4[redacted]
Passphrase	•••••
Confirm Passphrase	•••••
Contact Name	
Contact E-Mail	

4.2.11.2 Certificates Upload

- Navigate: **TLS management > Certificates**. Click **Install**
- Set Type: Select **CA Certificate**
- Set Name: **zoom1**
- Set Allow weak Certificate/Key: **checked**
- Set Certificate File: Click Choose File to select DigiCertGlobal1.crt.pem
- Click **Upload**



Install Certificate

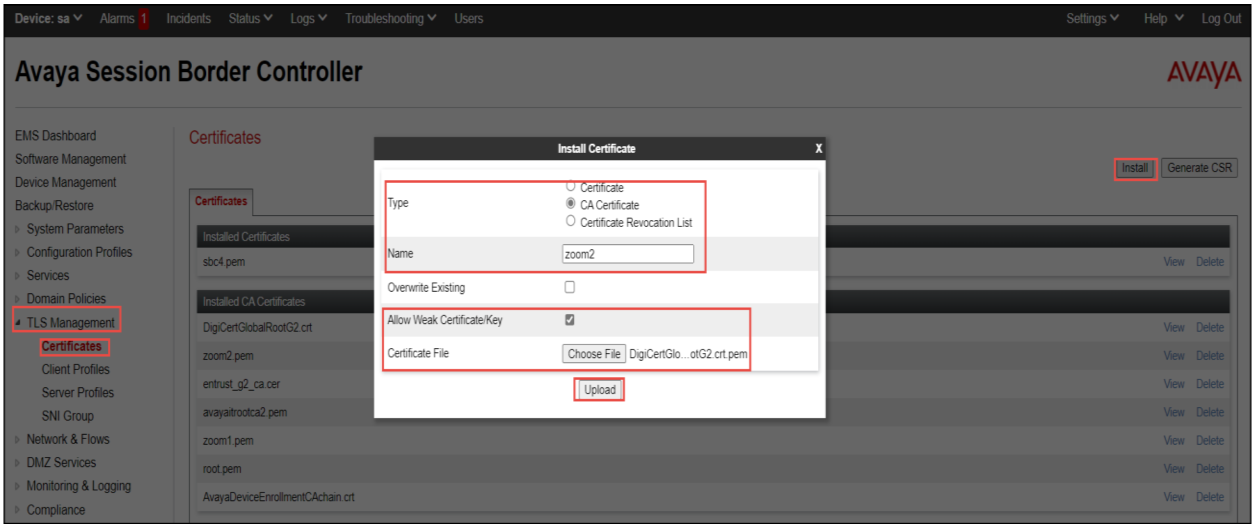
Type	○ Certificate ● CA Certificate ○ Certificate Revocation List
Name	zoom1
Overwrite Existing	□
Allow Weak Certificate/Key	☑
Certificate File	Choose File DigiCertGlobal1.crt.pem

Upload

Installed Certificates
sbc4.pem

Installed CA Certificates
DigiCertGlobalRootG2.crt
zoom2.pem
entrust_g2_ca.cer
avayaitrootca2.pem
zoom1.pem
root.pem
AvayaDeviceEnrollmentCAchain.crt

- Navigate: **TLS management > Certificates**. Click **Install**
- Set Type: Select **CA Certificate**
- Set Name: **zoom2**
- Set Allow weak Certificate/Key: **checked**
- Set Certificate File: Click Choose File to select **DigiCertGlobalRootG2.crt.pem**
- Click **Upload**



Install Certificate

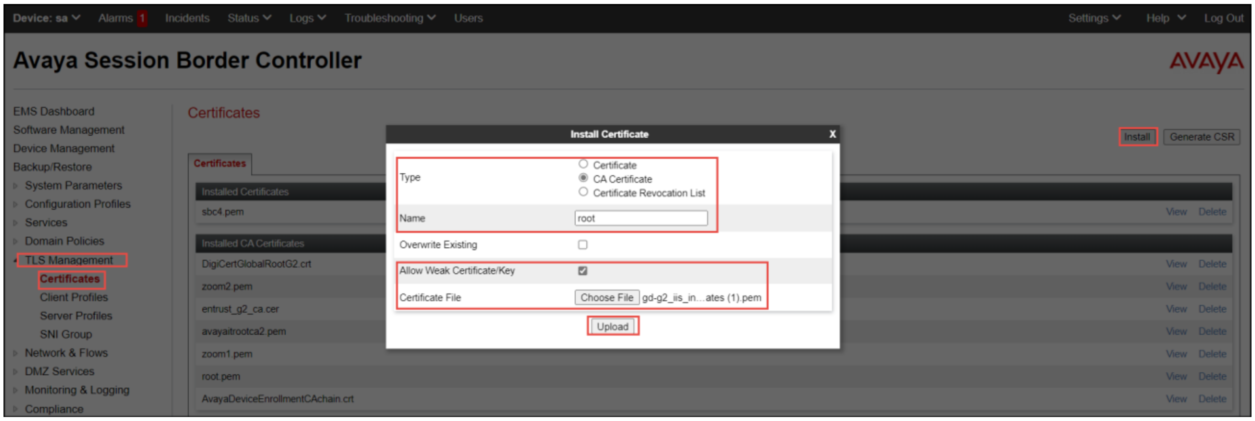
Type	○ Certificate ● CA Certificate ○ Certificate Revocation List
Name	zoom2
Overwrite Existing	□
Allow Weak Certificate/Key	☑
Certificate File	Choose File DigiCertGlo...otG2.crt.pem

Upload

Installed Certificates
sbc4.pem

Installed CA Certificates
DigiCertGlobalRootG2.crt
zoom2.pem
entrust_g2_ca.cer
avayaitrootca2.pem
zoom1.pem
root.pem
AvayaDeviceEnrollmentCAchain.crt

- Set **Type**: Select **CA Certificate**
- Set Name: **root** (i:e Go daddy intermediate certificate)
- Set Allow weak Certificate/Key: **checked**
- Set Certificate File: Click Choose File to select **gd-g2_iis_intermediates.pem**
- Click **Upload**



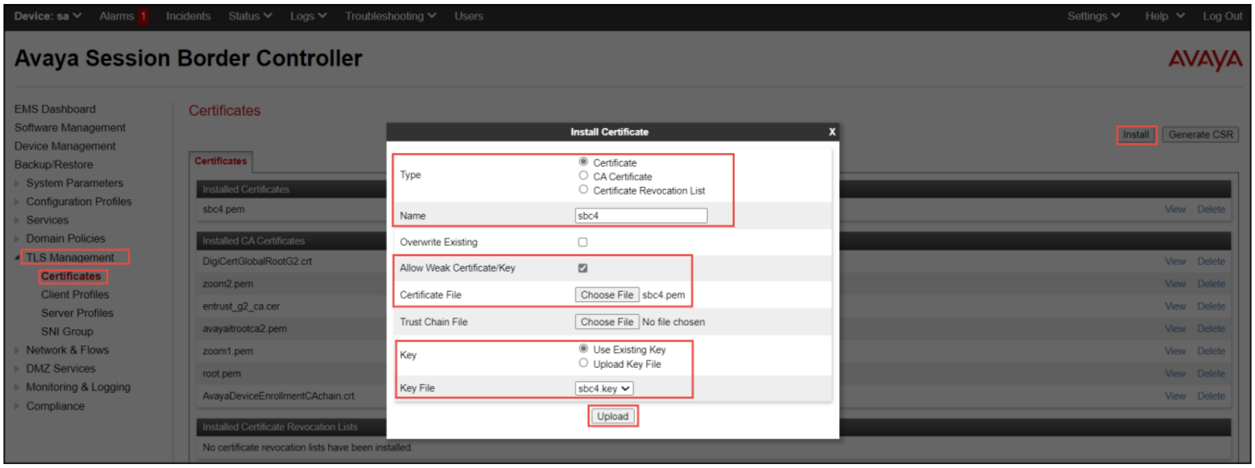
Install Certificate

Type	○ Certificate ● CA Certificate ○ Certificate Revocation List
Name	root
Overwrite Existing	□
Allow Weak Certificate/Key	☑
Certificate File	gd-g2_iis_in...ates (1).pem

Installed Certificates: sbc4.pem

Installed CA Certificates: DigiCertGlobalRootG2.crt, zoom2.pem, entrust_g2_ca.cer, avayaitrootca2.pem, zoom1.pem, root.pem, AvayaDeviceEnrollmentCAchain.crt

- Navigate: **TLS management > Certificates**. Click **Install**
- Set Type: Select **Certificate**
- Set Name: **sbc4**
- Set Allow weak Certificate/Key: **Checked**
- Set Certificate File: Click Choose File to select **sbc4.pem**
- Set **Key: Use Existing Key**
- Select **Key file: sbc4.key**
- Click **Upload**



Install Certificate

Type	● Certificate ○ CA Certificate ○ Certificate Revocation List
Name	sbc4
Overwrite Existing	□
Allow Weak Certificate/Key	☑
Certificate File	sbc4.pem
Trust Chain File	No file chosen
Key	● Use Existing Key ○ Upload Key File
Key File	sbc4.key

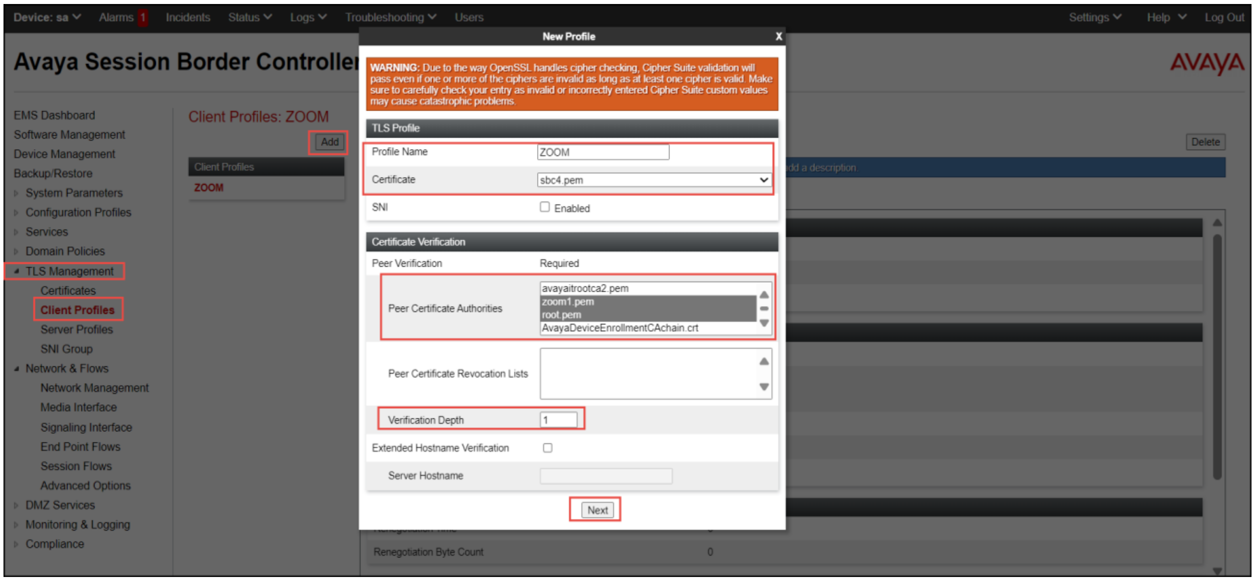
Installed Certificates: sbc4.pem

Installed CA Certificates: DigiCertGlobalRootG2.crt, zoom2.pem, entrust_g2_ca.cer, avayaitrootca2.pem, zoom1.pem, root.pem, AvayaDeviceEnrollmentCAchain.crt

No certificate revocation lists have been installed.

4.2.11.3 Client Profile

- Navigate to **TLS management > Client Profiles** and Click **Add**
- **Set Profile Name: ZOOM** is given for interface facing **ZOOM PBX**
- Set **Certificate**: Select server certificate **sbc4.pem** for Avaya SBC interface facing ZOOM PBX
- Set **Peer Certificate Authorities**: Select **zoom1.pem, zoom2.pem, root.pem** which is uploaded in previous step
- Set **Verification Depth: 1**
- Click **Next**



WARNING: Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.

TLS Profile

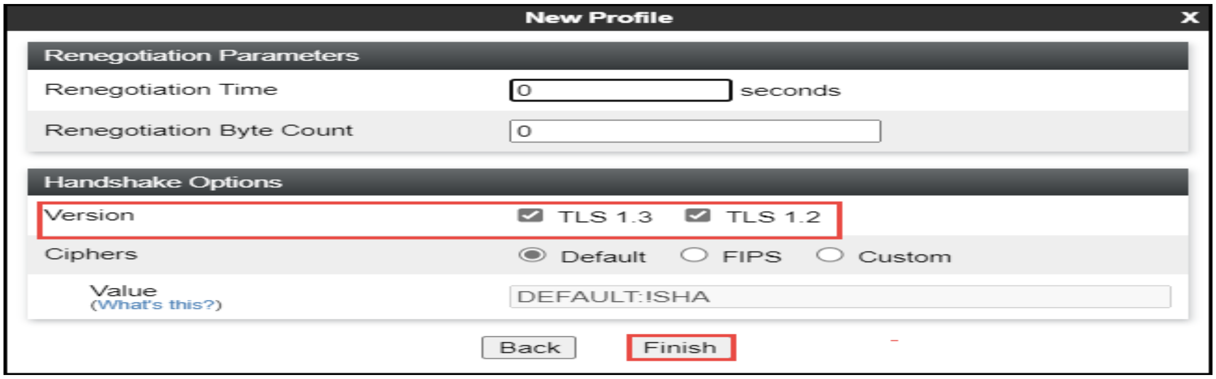
Profile Name	ZOOM
Certificate	sbc4.pem
SNI	☐ Enabled

Certificate Verification

Peer Verification	Required
Peer Certificate Authorities	avayaitrootca2.pem zoom1.pem root.pem AvayaDeviceEnrollmentCAchain.crt
Peer Certificate Revocation Lists	
Verification Depth	1
Extended Hostname Verification	☐
Server Hostname	

Renegotiation Byte Count 0

- Set **Version**: Select **TLS 1.2, TLS 1.3** versions
- Click **Finish**



Renegotiation Parameters

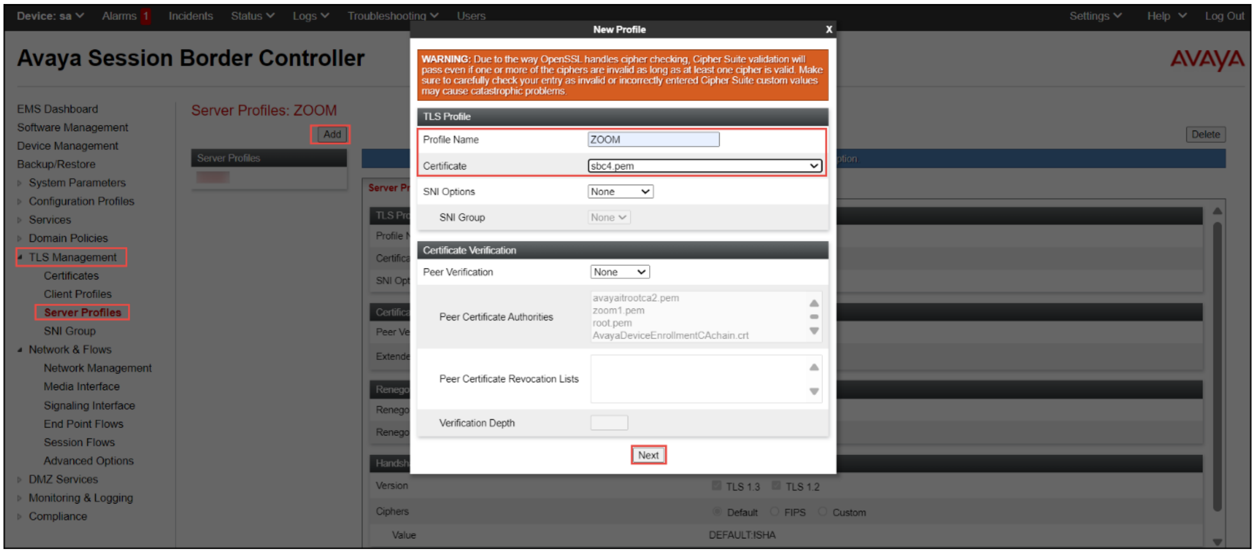
Renegotiation Time	0 seconds
Renegotiation Byte Count	0

Handshake Options

Version	☑ TLS 1.3 ☑ TLS 1.2
Ciphers	● Default ○ FIPS ○ Custom
Value (What's this?)	DEFAULT:!SHA

4.2.11.4 Server Profile

- Navigate: **TLS management > Server Profiles**. Click **Add**
- Set Profile Name: **ZOOM** is given for interface facing Zoom
- Set Certificate: Select server certificate **sbc4.pem** for Avaya SBC interface facing ZOOM
- Click on **Next**



New Profile

WARNING: Due to the way OpenSSL handles cipher checking, Cipher Suite validation will pass even if one or more of the ciphers are invalid as long as at least one cipher is valid. Make sure to carefully check your entry as invalid or incorrectly entered Cipher Suite custom values may cause catastrophic problems.

TLS Profile

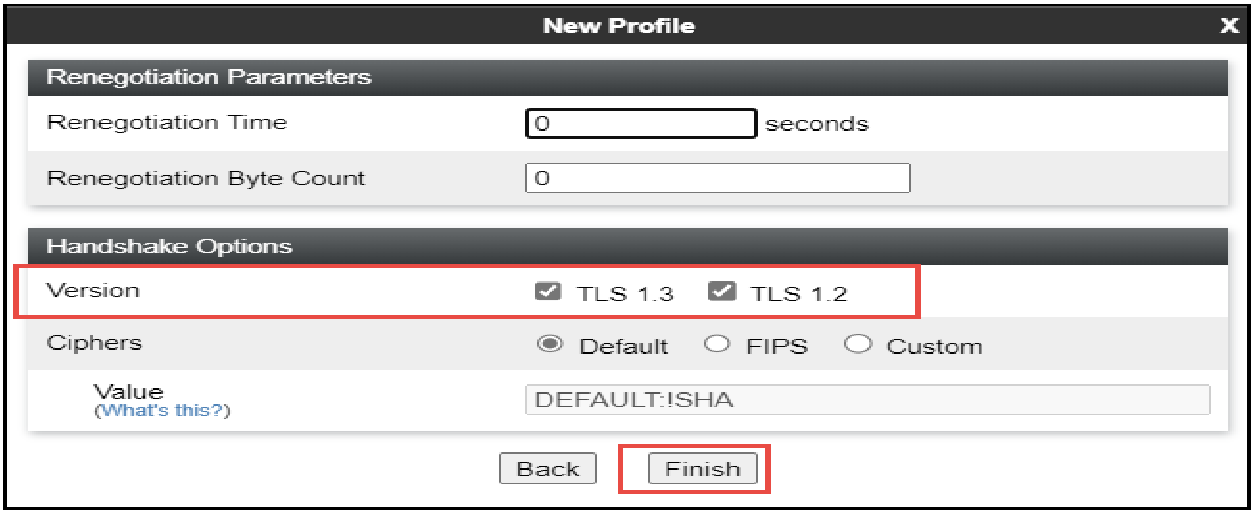
Profile Name	ZOOM
Certificate	sbc4.pem
SNI Options	None
SNI Group	None

Certificate Verification

Peer Verification	None
Peer Certificate Authorities	avayaitrootca2.pem zoom1.pem root.pem AvayaDeviceEnrollmentCAchain.crt
Peer Certificate Revocation Lists	
Verification Depth	

Next

- Set Version: Select **TLS 1.2, TLS 1.3** versions
- Click **Finish**



New Profile

Renegotiation Parameters

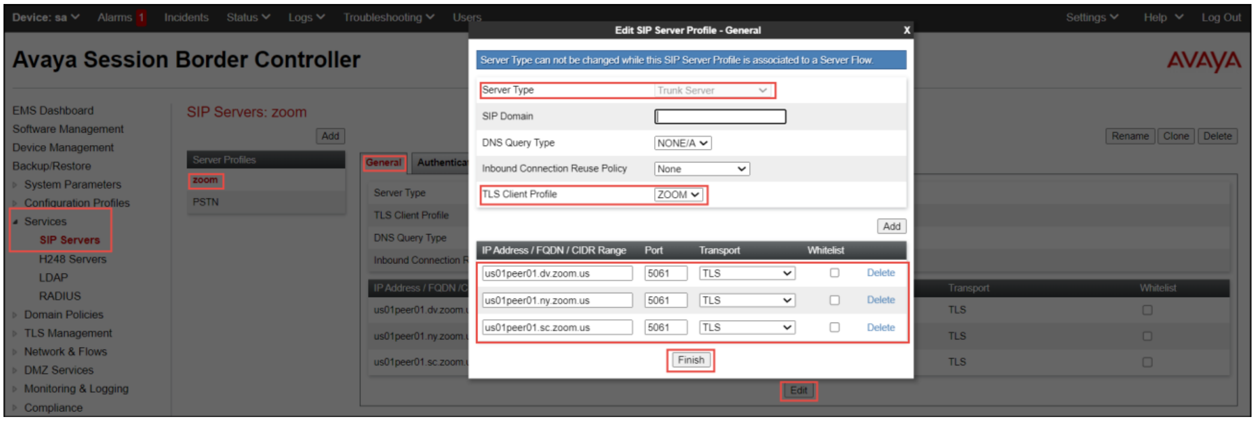
Renegotiation Time	0 seconds
Renegotiation Byte Count	0

Handshake Options

Version	☑ TLS 1.3 ☑ TLS 1.2
Ciphers	● Default ○ FIPS ○ Custom
Value (What's this?)	DEFAULT:!SHA

Edit **SIP Server**

- Navigate to **Services > SIP Servers**
- Select Server Profiles: **zoom**
- Under **General** tab and Click **Edit**
- Set Server Type: Select **Trunk Server** from the drop down
- Set TLS Client Profile: **ZOOM**
- Set IP Address/FQDN/CIDR Range: Enter the ZOOM PBX FQDN's
- Set Transport: Select **TLS** from Dropdown
- Set Port: **5061**
- Set TLS Client Profile: Select Client Profile **ZOOM**
- Click **Finish**



Edit SIP Server Profile - General

Server Type can not be changed while this SIP Server Profile is associated to a Server Flow.

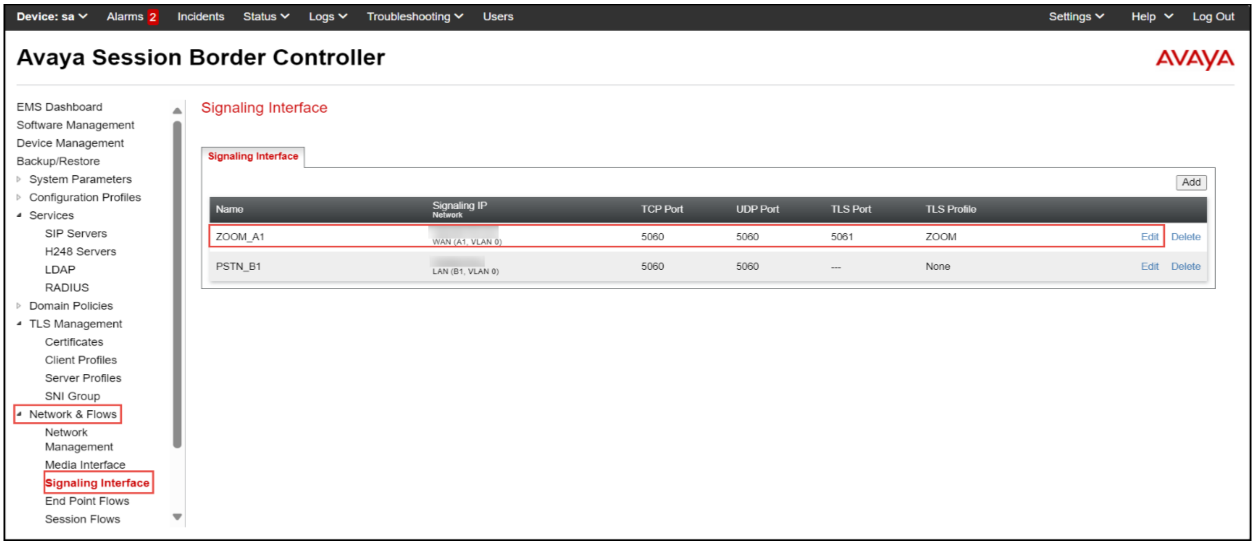
Server Type	Trunk Server
SIP Domain	
DNS Query Type	NONE/A
Inbound Connection Reuse Policy	None
TLS Client Profile	ZOOM

IP Address / FQDN / CIDR Range	Port	Transport	Whitelist	
us01peer01.dv.zoom.us	5061	TLS	□	Delete
us01peer01.ny.zoom.us	5061	TLS	□	Delete
us01peer01.sc.zoom.us	5061	TLS	□	Delete

Finish

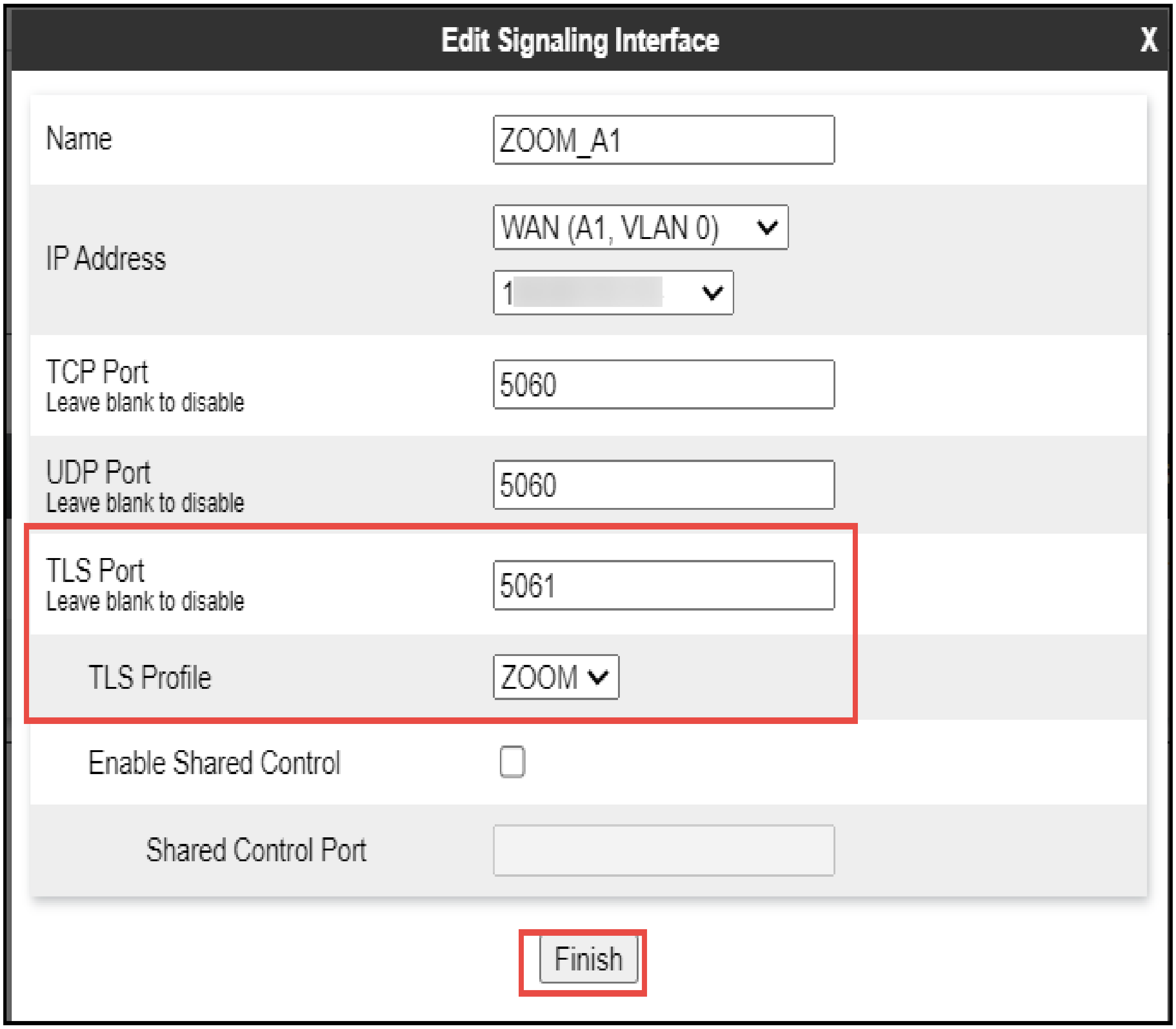
Edit **Signaling Interface**

- Navigate to **Network & Flows > Signaling Interface**
- Select interface **ZOOM_A1**
- Click **Edit**



Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile		
ZOOM_A1	[redacted] WAN (A1, VLAN 0)	5060	5060	5061	ZOOM	Edit	Delete
PSTN_B1	[redacted] LAN (B1, VLAN 0)	5060	5060	---	None	Edit	Delete

- Set TLS Port: **5061.**
- Set TLS Profile: Select **ZOOM** from the drop-down menu.
- Click **Finish.**



Edit Signaling Interface

Name	ZOOM_A1
IP Address	WAN (A1, VLAN 0) 1[redacted]
TCP Port Leave blank to disable	5060
UDP Port Leave blank to disable	5060
TLS Port Leave blank to disable	5061
TLS Profile	ZOOM
Enable Shared Control	□
Shared Control Port	

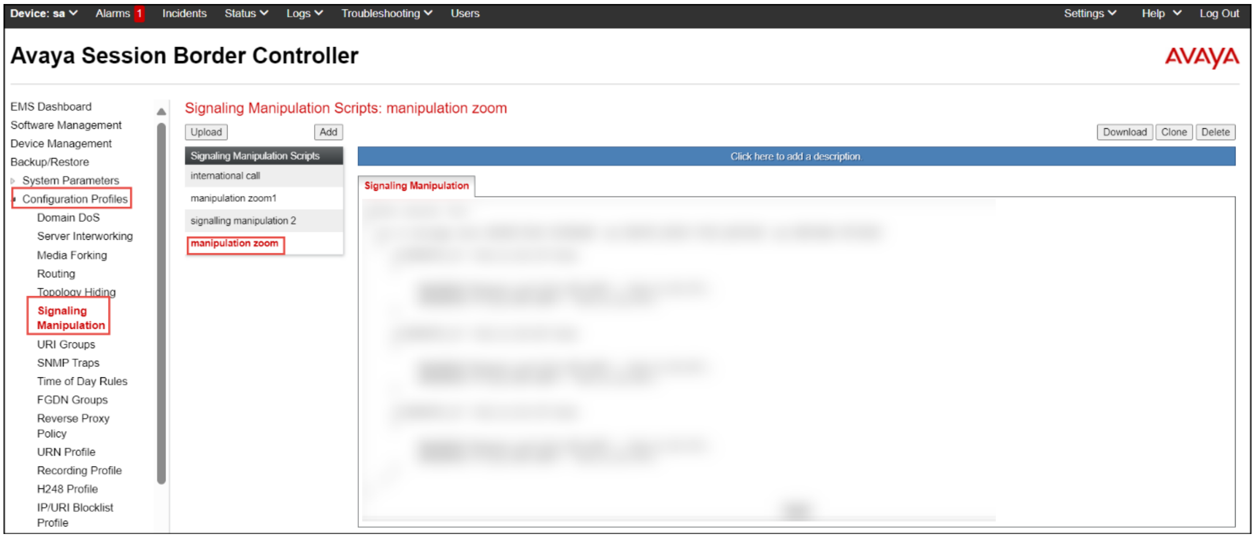
4.2.12 Signaling Manipulation

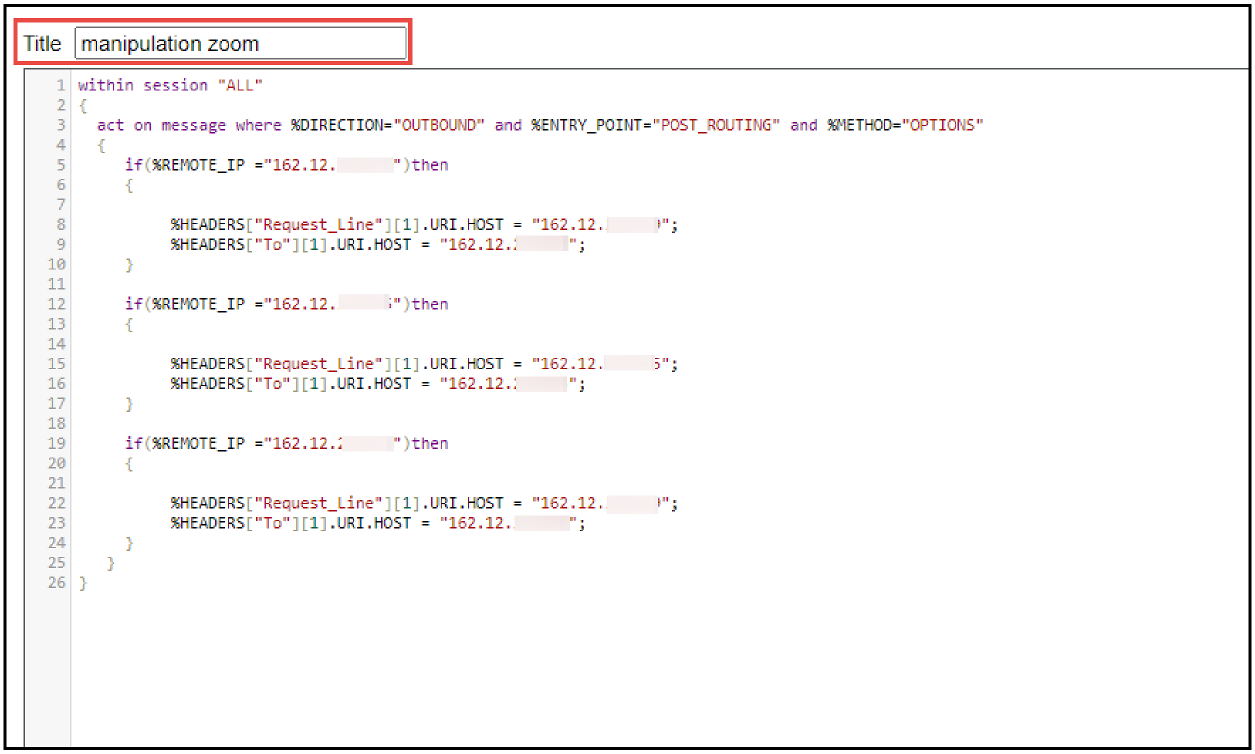
The signaling manipulation feature provides the ability to add, change and delete any of the headers and other information in SIP messages. This feature addresses the interop issues.

4.2.12.1 SIP OPTIONS URI Manipulation

Zoom PBX expecting the request URI and To URI with resolved IP address of configured FQDN for OPTIONS heartbeat request, below sigma script is created to send OPTIONS message with resolved IP address of Zoom PBX. (Refer 4.2.10 End point Flow)

- Navigate to **Configuration Profiles** > **Signaling Manipulation** > **manipulation zoom**
- Below is the **"manipulation zoom"** script that is used in this test





Title manipulation zoom

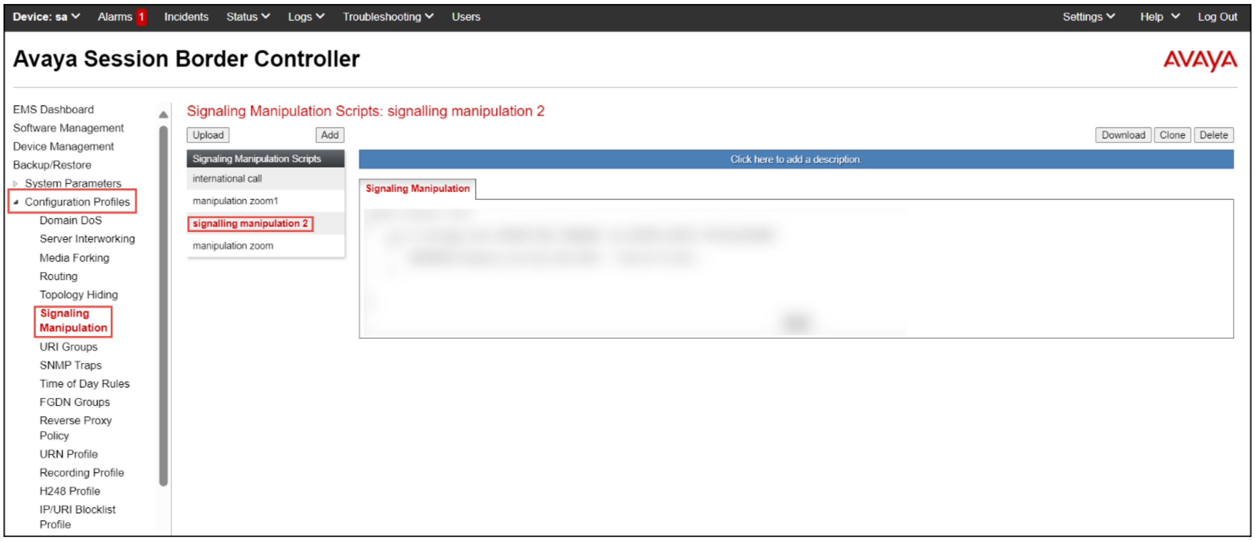
```
within session "ALL"
{
  act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING" and %METHOD="OPTIONS"
  {
     if(%REMOTE_IP ="162.12.[redacted]")then
     {

          %HEADERS["Request_Line"][1].URI.HOST = "162.12.[redacted]";
          %HEADERS["To"][1].URI.HOST = "162.12.[redacted]";
     }

     if(%REMOTE_IP ="162.12.[redacted]")then
     {

          %HEADERS["Request_Line"][1].URI.HOST = "162.12.[redacted]";
          %HEADERS["To"][1].URI.HOST = "162.12.[redacted]";
     }

     if(%REMOTE_IP ="162.12.[redacted]")then
     {

          %HEADERS["Request_Line"][1].URI.HOST = "162.12.[redacted]";
          %HEADERS["To"][1].URI.HOST = "162.12.[redacted]";
     }
   }
}
```

```
within session "ALL"

{

act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING" and
%METHOD="OPTIONS"

{

if(%REMOTE_IP ="162.12.XX.XX")then

{


%HEADERS["Request_Line"][1].URI.HOST = "162.12.XX.XX";

%HEADERS["To"][1].URI.HOST = "162.12.XX.XX";

}


if(%REMOTE_IP ="162.12.XX.XX")then

{


%HEADERS["Request_Line"][1].URI.HOST = "162.12.XX.XX";

                              %HEADERS["To"][1].URI.HOST = "162.12.XX.XX";

                                                            }


if(%REMOTE_IP ="162.12.XXX.XX")then

                                                            {


%HEADERS["Request_Line"][1].URI.HOST = "162.12.XX.XX";

                              %HEADERS["To"][1].URI.HOST = "162.12.XX.XX";

                                                            }

                                                            }

                                                            }
```

4.2.12.2 FQDN to IP Translation

Avaya SBC uses SIGMA configuration to translate the FQDN to its IP address at the ingress. This translation is required for all In-dialog requests coming from Zoom. Without this SIGMA properly configured, In-dialog request coming from Zoom would be rejected with appropriate error response. For an example, in a Zoom to PSTN active call through Avaya SBC, In-Dialog request BYE coming from Zoom to terminate the call will be rejected, caused the SIP session towards PSTN will remain active until it is disconnected by the PSTN user. (Refer 4.2.2 SIP Server)

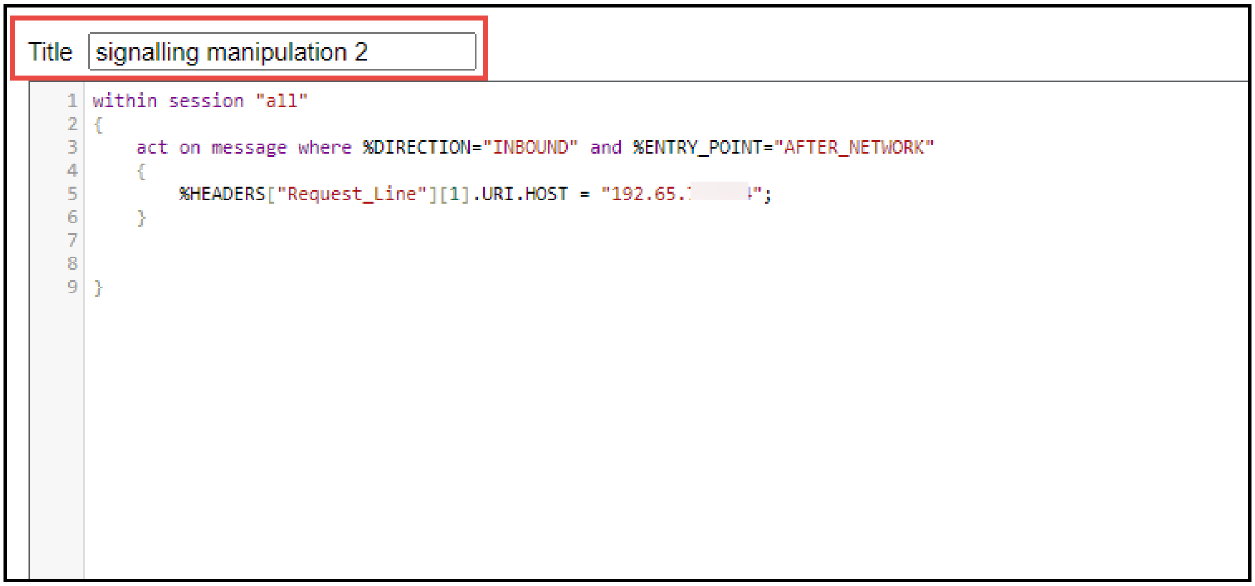
- Navigate to **Configuration Profiles > Signaling Manipulation > signaling manipulation 2**
- Below is the **"signaling manipulation 2"** script that is used in this test



Avaya Session Border Controller

Signaling Manipulation Scripts: signalling manipulation 2

[redacted]



Title signalling manipulation 2

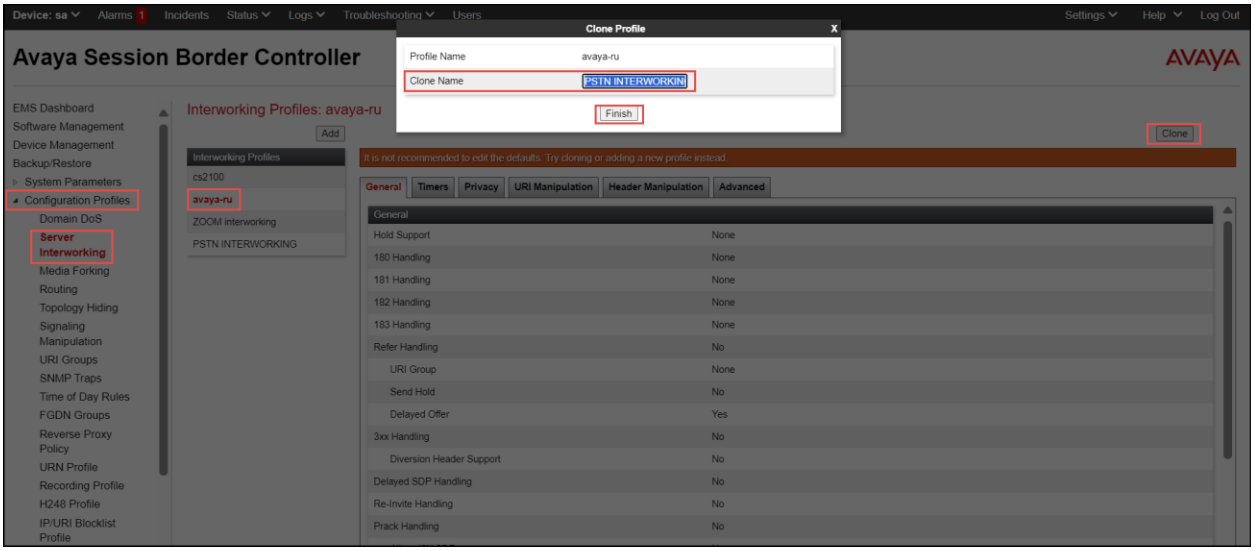
```
within session "all"
{
    act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
    {
        %HEADERS["Request_Line"][1].URI.HOST = "192.65.[redacted]";
    }


}
```

```
within session "all"
{
   act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
   {
      %HEADERS["Request_Line"][1]. URI.HOST = "192.65.XX.XX";
   }



}
```

4.3 PSTN Leg Configuration

4.3.1 Server Interworking for PSTN Gateway

- Navigate to **Configuration Profiles > Server Interworking**
- Select the default Interworking Profile **avaya-ru**, click **Clone**
- Set Clone Name: **PSTN INTERWORKING**
- Click **Finish**



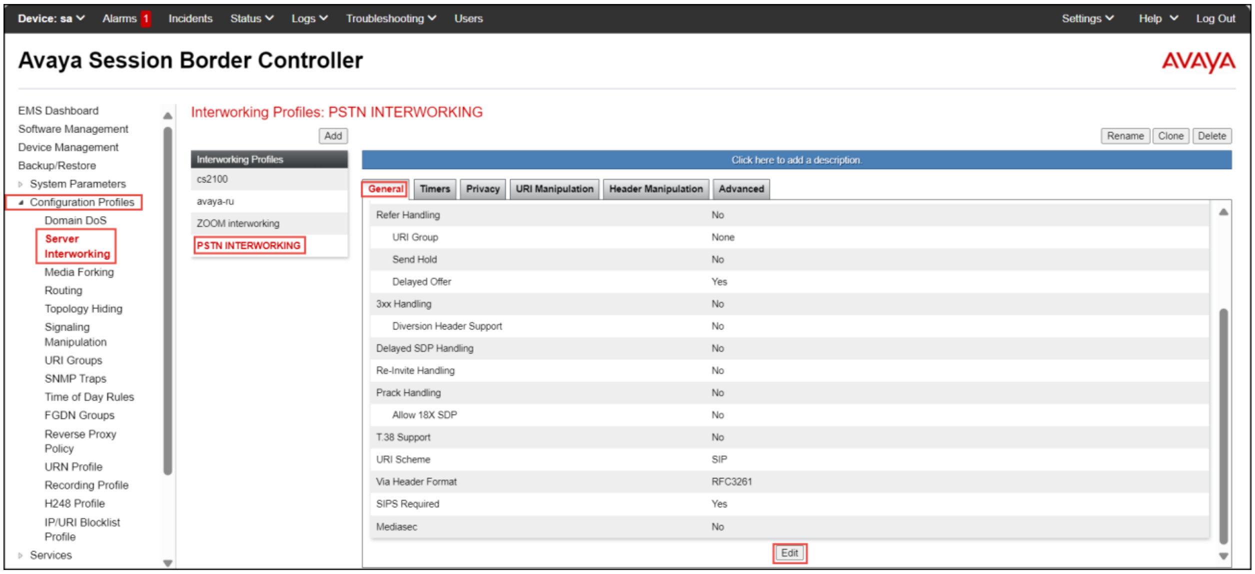
Clone Profile

Profile Name	avaya-ru
Clone Name	PSTN INTERWORKIN

It is not recommended to edit the defaults. Try cloning or adding a new profile instead.

General	
Hold Support	None
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	Yes
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No

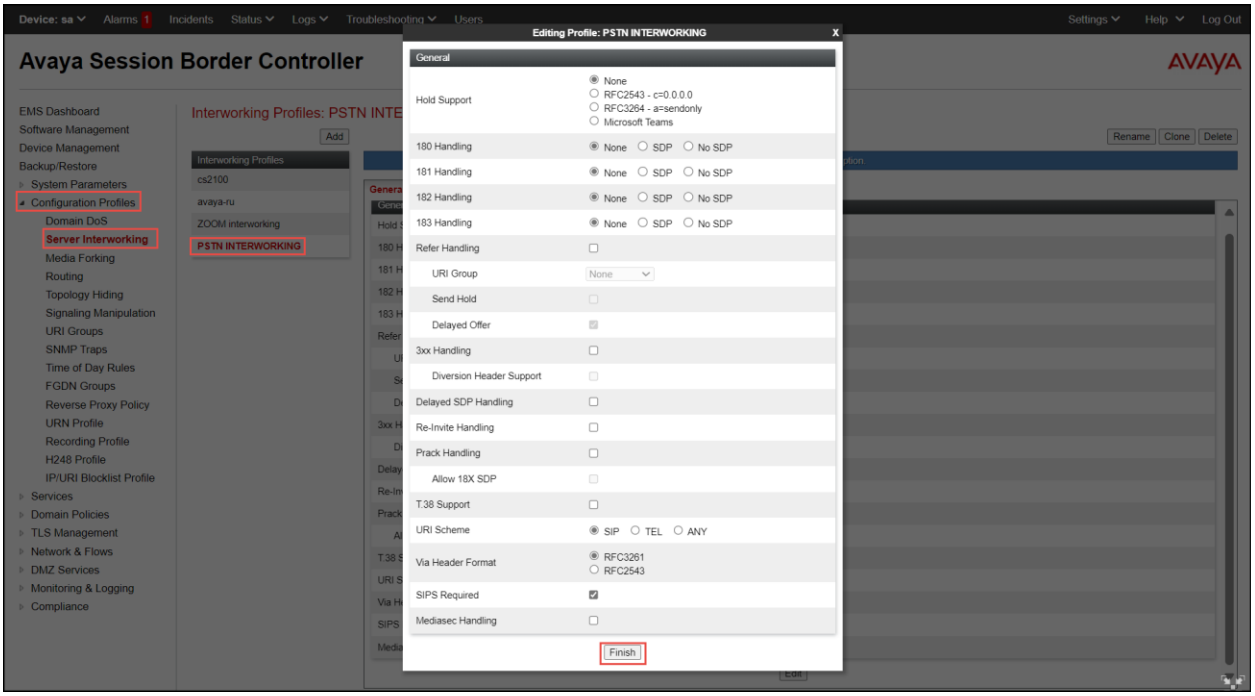
- Select **Server Interworking: PSTN INTERWORKING**
- Select **General** tab and click **Edit**



Interworking Profiles: PSTN INTERWORKING

Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	Yes
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261
SIPS Required	Yes
Mediasec	No

- All the parameters are set to default, refer the below figure
- Click on **Finish**

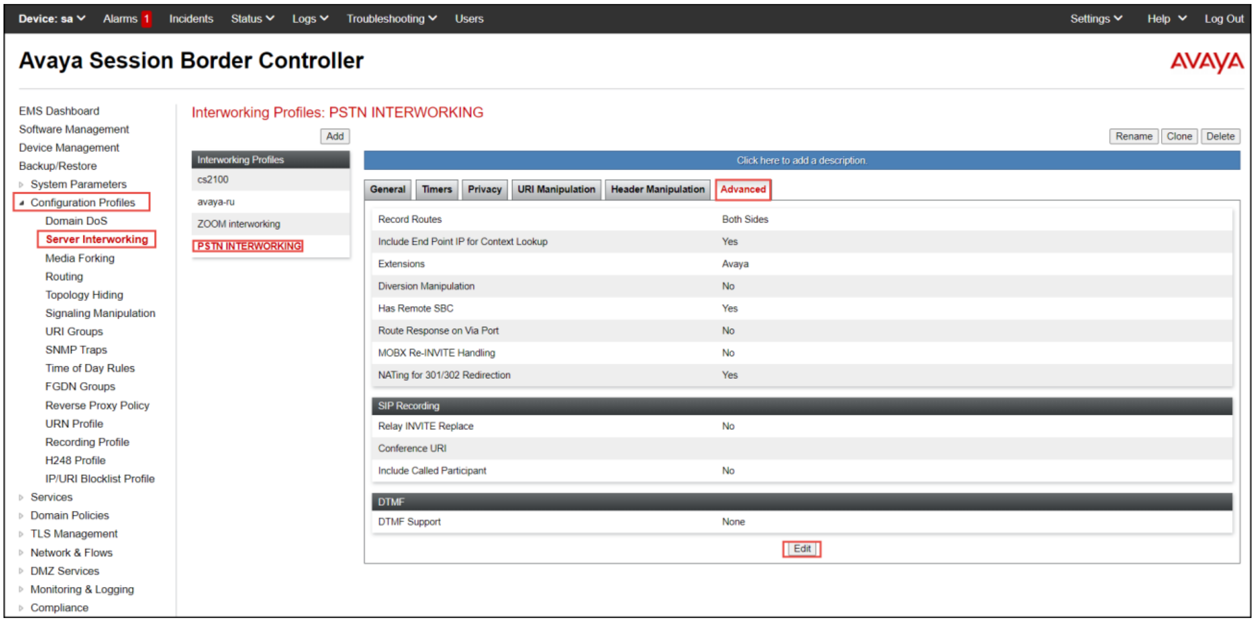


Editing Profile: PSTN INTERWORKING

General

Hold Support	● None ○ RFC2543 - c=0.0.0.0 ○ RFC3264 - a=sendonly ○ Microsoft Teams
180 Handling	● None ○ SDP ○ No SDP
181 Handling	● None ○ SDP ○ No SDP
182 Handling	● None ○ SDP ○ No SDP
183 Handling	● None ○ SDP ○ No SDP
Refer Handling	□
URI Group	None
Send Hold	□
Delayed Offer	☑
3xx Handling	□
Diversion Header Support	□
Delayed SDP Handling	□
Re-Invite Handling	□
Prack Handling	□
Allow 18X SDP	□
T.38 Support	□
URI Scheme	● SIP ○ TEL ○ ANY
Via Header Format	● RFC3261 ○ RFC2543
SIPS Required	☑
Mediasec Handling	□

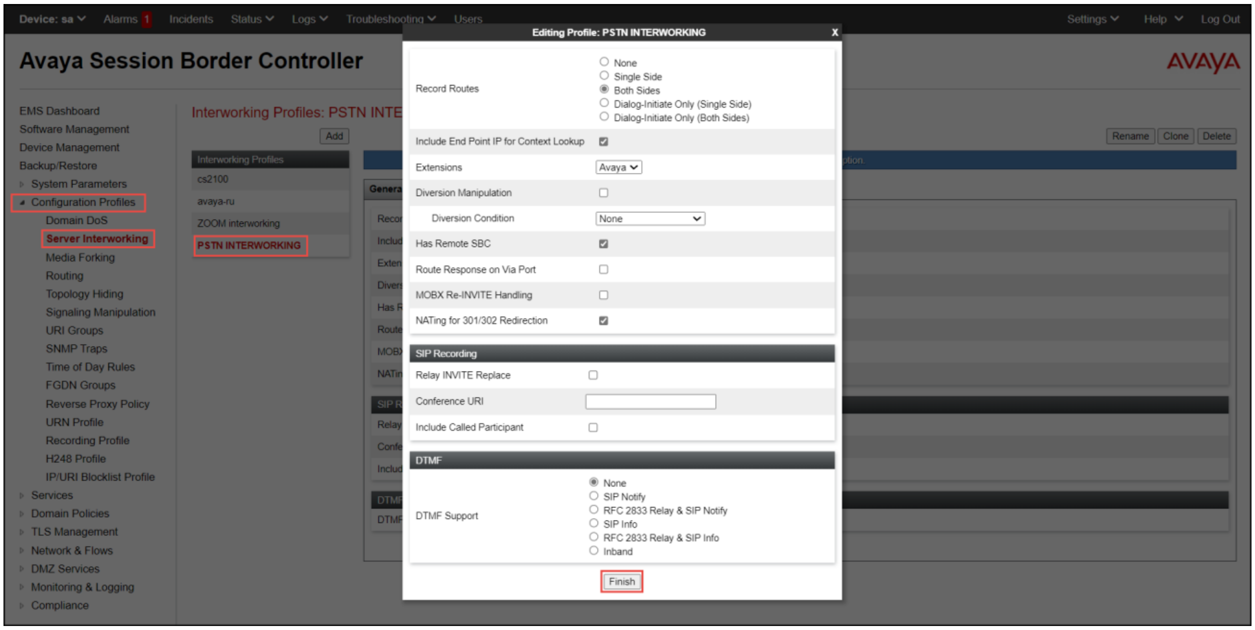
- Select **Advanced** tab and click **Edit**



Interworking Profiles: PSTN INTERWORKING

Record Routes	Both Sides
Include End Point IP for Context Lookup	Yes
Extensions	Avaya
Diversion Manipulation	No
Has Remote SBC	Yes
Route Response on Via Port	No
MOBX Re-INVITE Handling	No
NATing for 301/302 Redirection	Yes
SIP Recording	
Relay INVITE Replace	No
Conference URI	
Include Called Participant	No
DTMF	
DTMF Support	None

- All the parameters are set to default, refer the below figure
- Click on **Finish**

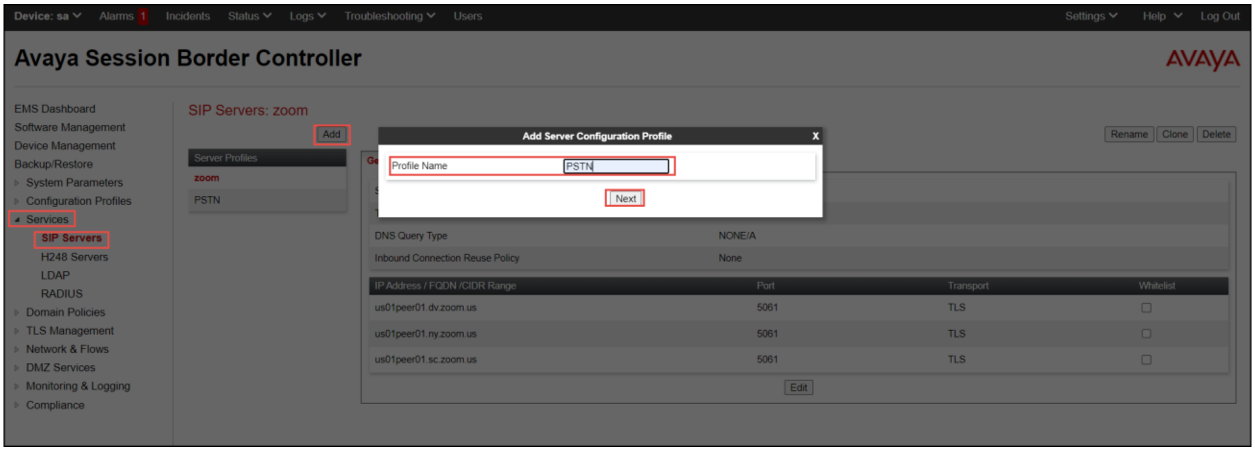


Editing Profile: PSTN INTERWORKING

Record Routes	○ None ○ Single Side ● Both Sides ○ Dialog-Initiate Only (Single Side) ○ Dialog-Initiate Only (Both Sides)
Include End Point IP for Context Lookup	☑
Extensions	Avaya
Diversion Manipulation	□
Diversion Condition	None
Has Remote SBC	☑
Route Response on Via Port	□
MOBX Re-INVITE Handling	□
NATing for 301/302 Redirection	☑
SIP Recording	
Relay INVITE Replace	□
Conference URI	
Include Called Participant	□
DTMF	
DTMF Support	● None ○ SIP Notify ○ RFC 2833 Relay & SIP Notify ○ SIP Info ○ RFC 2833 Relay & SIP Info ○ Inband

4.3.2 SIP Server

- Navigate to **Services > SIP Servers**
- Click **Add**
- Set Profile Name: **PSTN**
- Click **Next**



Add Server Configuration Profile

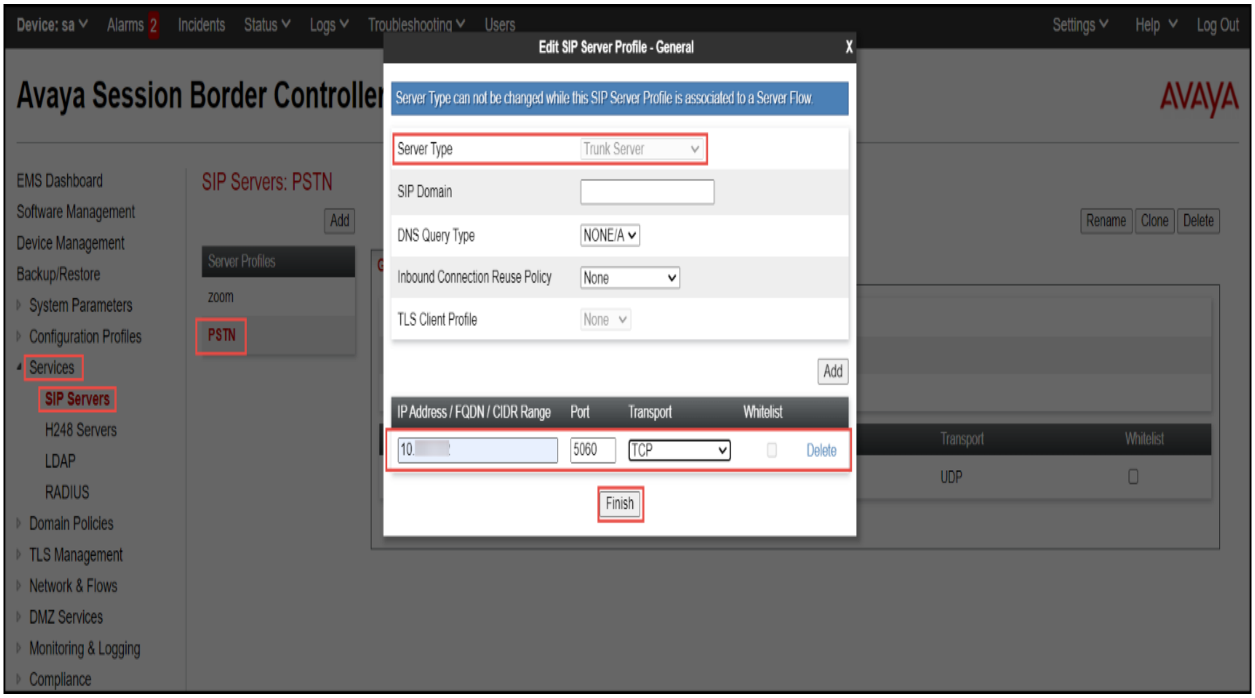
Profile Name: PSTN

Next

DNS Query Type	NONE/A
Inbound Connection Reuse Policy	None

IP Address / FQDN /CIDR Range	Port	Transport	Whitelist
us01peer01.dv.zoom.us	5061	TLS	□
us01peer01.ny.zoom.us	5061	TLS	□
us01peer01.sc.zoom.us	5061	TLS	□

- Set Server Type: Select **Trunk Server** from the drop down
- Set IP Address/FQDN/CIDR Range: Enter the **PSTN Gateway IP address**
- Set Port: **5060**
- Set Transport: **TCP**
- Click **Finish**



Edit SIP Server Profile - General

Server Type can not be changed while this SIP Server Profile is associated to a Server Flow.

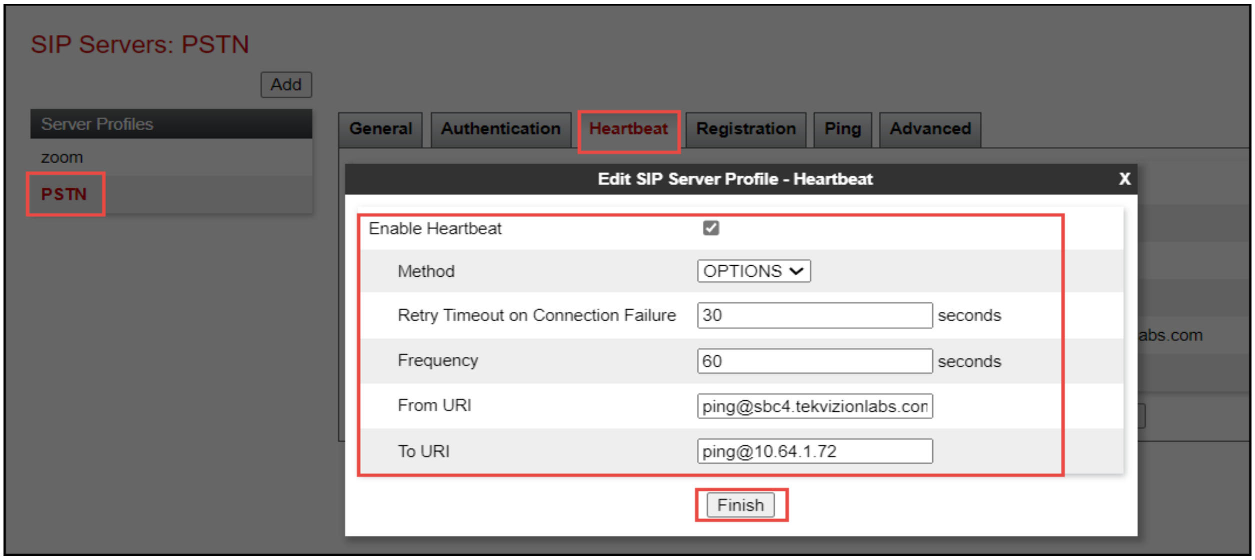
Server Type	Trunk Server
SIP Domain	
DNS Query Type	NONE/A
Inbound Connection Reuse Policy	None
TLS Client Profile	None

Add

IP Address / FQDN / CIDR Range	Port	Transport	Whitelist	
10.[redacted]	5060	TCP	□	Delete

Finish

- Navigate to **Heartbeat** tab
- Set Enable Heartbeat: **Checked**
- Set Method: **OPTIONS**
- Set Retry Timeout on Connection Failure**: 30 seconds**
- Set Frequency: **60 seconds**
- Set From URI: **ping@<Signaling Interface IP of PSTN Gateway>**
- Set To URI: **ping@< PSTN Gateway IP>**
- Click **Finish**

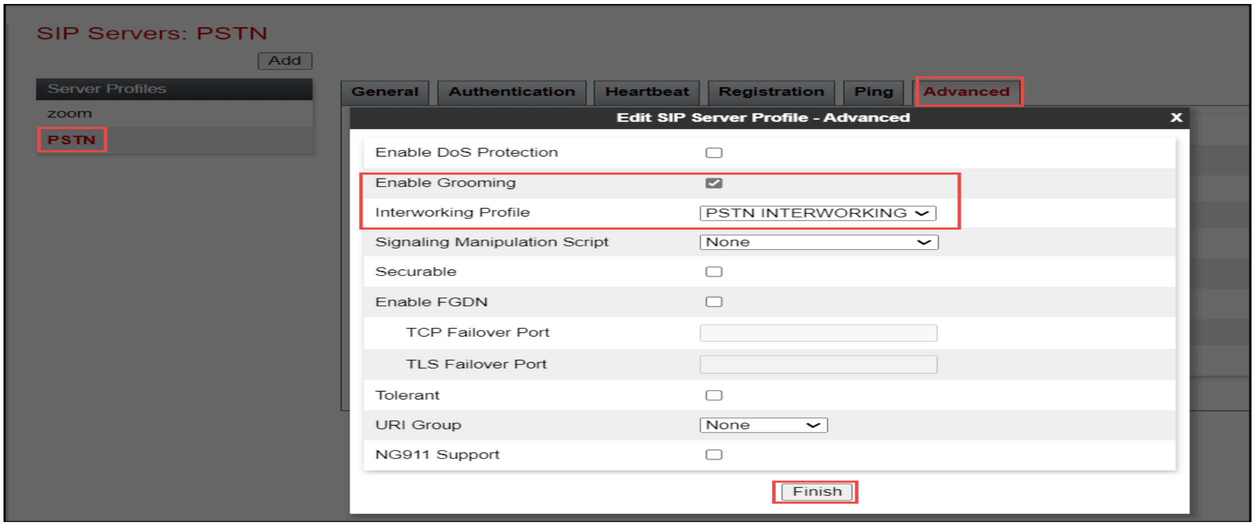


SIP Servers: PSTN

Edit SIP Server Profile - Heartbeat

Enable Heartbeat	☑
Method	OPTIONS
Retry Timeout on Connection Failure	30 seconds
Frequency	60 seconds
From URI	ping@sbc4.tekvizionlabs.con
To URI	ping@10.64.1.72

- Navigate to **Advanced** tab
- Enable Grooming: **Checked**
- Interworking Profile: Select **PSTN INTERWORKING**
- Click **Finish**



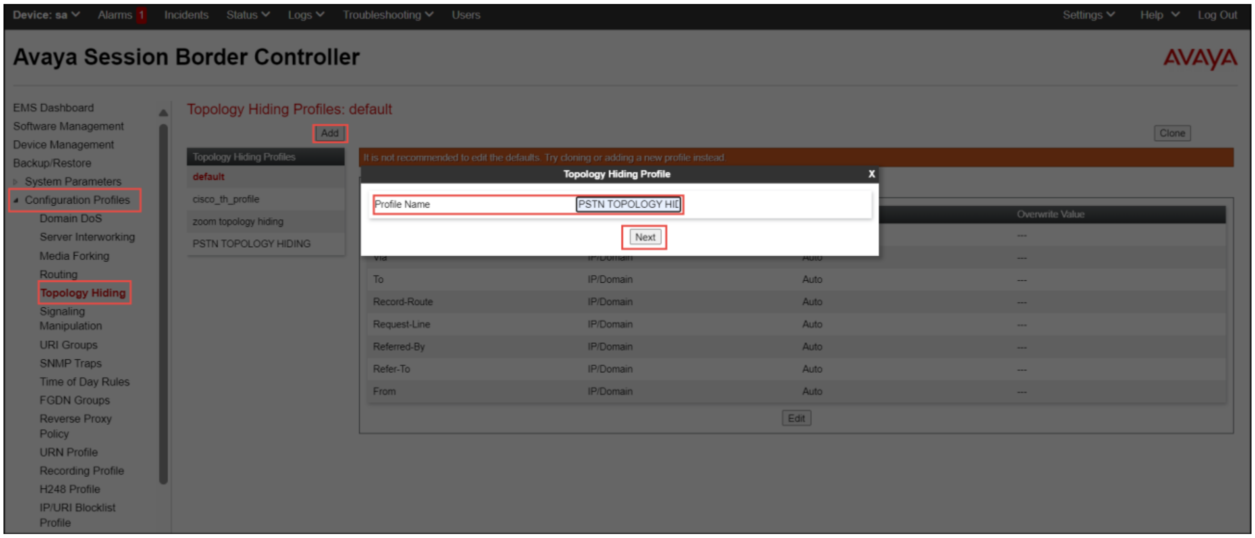
SIP Servers: PSTN

Edit SIP Server Profile - Advanced

Enable DoS Protection	☐
Enable Grooming	☑
Interworking Profile	PSTN INTERWORKING
Signaling Manipulation Script	None
Securable	☐
Enable FGDN	☐
TCP Failover Port	
TLS Failover Port	
Tolerant	☐
URI Group	None
NG911 Support	☐

4.3.3Topology Hiding

- Navigate to **Configuration Profiles** > **Topology Hiding**
- Click **Add**
- Set Profile Name: **PSTN TOPOLOGY HIDING**
- Click **Next**



Topology Hiding Profiles: default

It is not recommended to edit the defaults. Try cloning or adding a new profile instead.

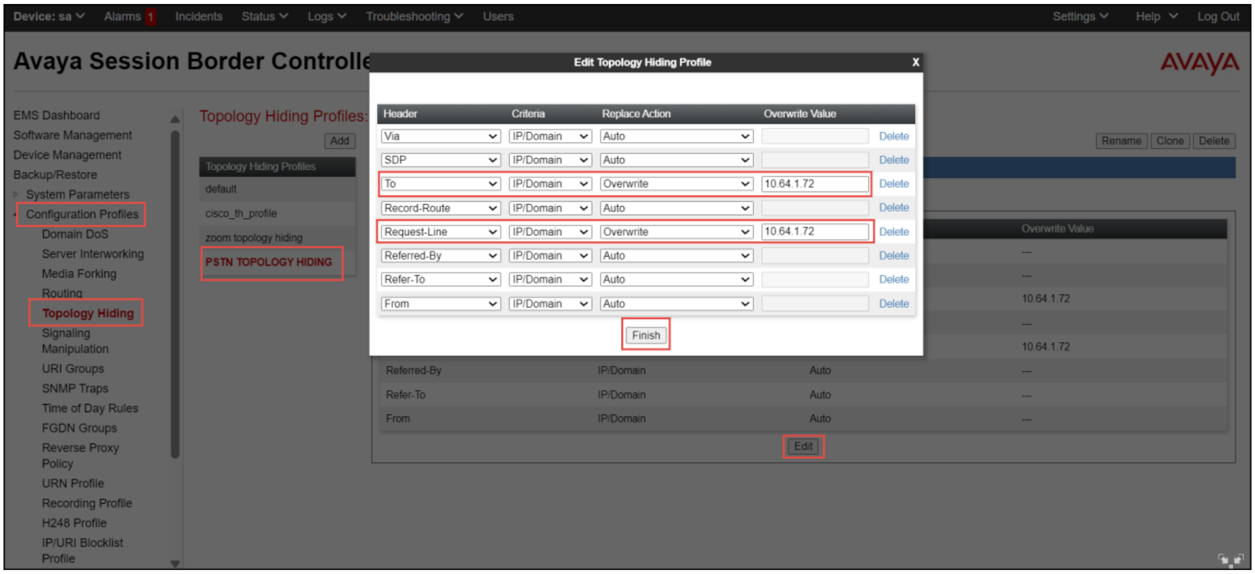
Topology Hiding Profile

Profile Name: PSTN TOPOLOGY HID

			Overwrite Value

Via	IP/Domain	Auto	---
To	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
Request-Line	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
From	IP/Domain	Auto	---

- Select the newly created profile **PSTN TOPOLOGY HIDING** and click **Edit**
- **Overwrite Value**: Replace the **Request-line** with PSTN facing IP
- **Overwrite Value**: Replace the **To** with PSTN facing IP
- Click **Finish**



Topology Hiding Profiles:

Edit Topology Hiding Profile

Header	Criteria	Replace Action	Overwrite Value	
Via	IP/Domain	Auto		Delete
SDP	IP/Domain	Auto		Delete
To	IP/Domain	Overwrite	10.64.1.72	Delete
Record-Route	IP/Domain	Auto		Delete
Request-Line	IP/Domain	Overwrite	10.64.1.72	Delete
Referred-By	IP/Domain	Auto		Delete
Refer-To	IP/Domain	Auto		Delete
From	IP/Domain	Auto		Delete

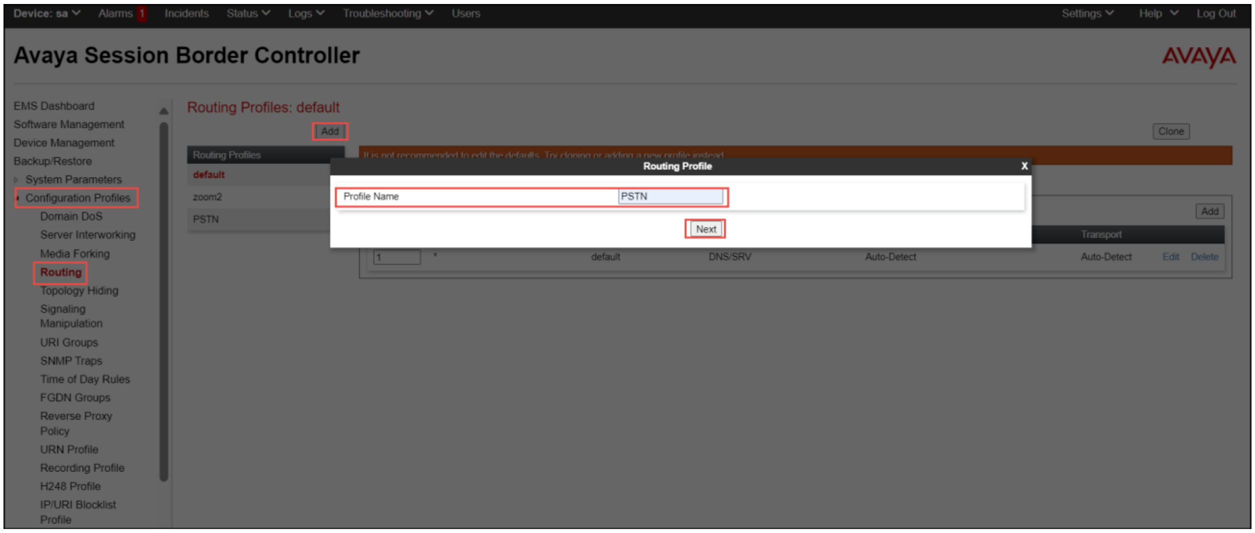
			Overwrite Value

			10.64.1.72

			10.64.1.72
Referred-By	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
From	IP/Domain	Auto	---

4.3.4 Routing

- Navigate to **Configuration Profiles** > **Routing**
- Click **Add**
- Set Profile Name: **PSTN**
- Click **Next**



Avaya Session Border Controller

Routing Profiles: default

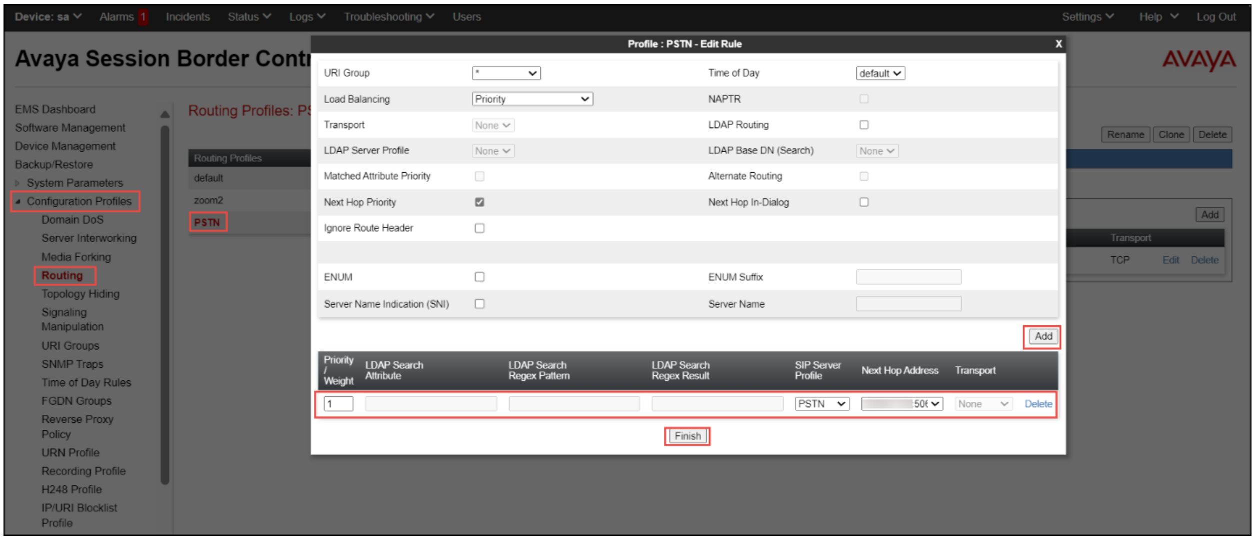
It is not recommended to edit the defaults. Try cloning or adding a new profile instead.

Routing Profile

Profile Name: PSTN

1 * default DNS/SRV Auto-Detect Auto-Detect

- At **Routing Profile** Window, Click **Add.**
- Set **Priority/Weight: 1**
- Select **SIP Server Profile: PSTN** from the drop-down menu
- Click **Finish**



Avaya Session Border Controller

Routing Profiles: PS

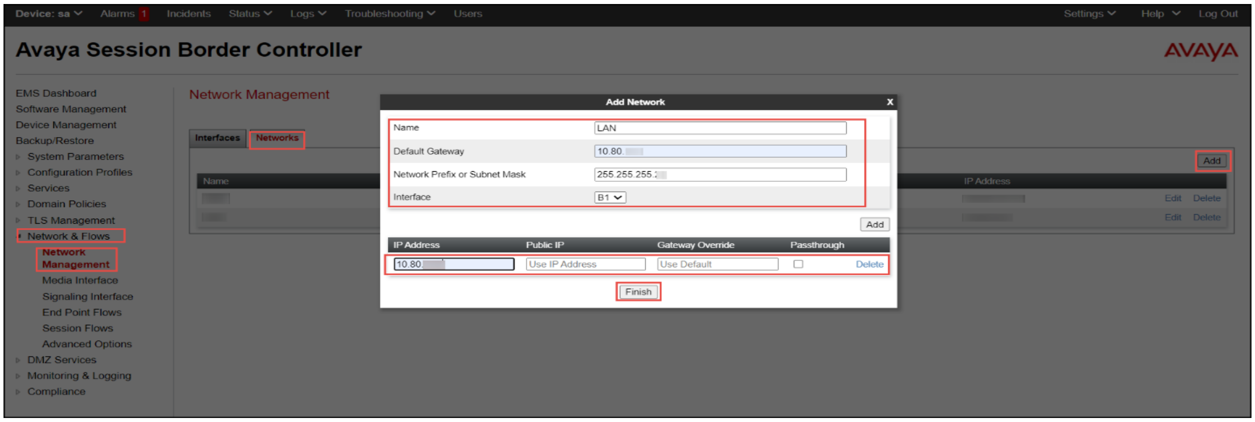
Profile : PSTN - Edit Rule

URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	□
Transport	None	LDAP Routing	□
LDAP Server Profile	None	LDAP Base DN (Search)	None
Matched Attribute Priority	□	Alternate Routing	□
Next Hop Priority	☑	Next Hop In-Dialog	□
Ignore Route Header	□		
ENUM	□	ENUM Suffix	
Server Name Indication (SNI)	□	Server Name	

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport
1				PSTN	[redacted]50(	None

4.3.5 Network Management

- Navigate to **Network & Flows > Network Management >Networks**
- Click **Add.** A window will appear titled **Add Network**
- Set Name: **LAN** is given for the network facing **PSTN gateway**
- Set **Default Gateway IP Address: 10.80.XX.X**
- Set **Network Prefix or Subnet Mask: 255.255.255.X**
- Set **Interface: B1**
- Set **IP Address** facing **PSTN Gateway: 10.80.XX.XX**
- Click **Finish**



Add Network

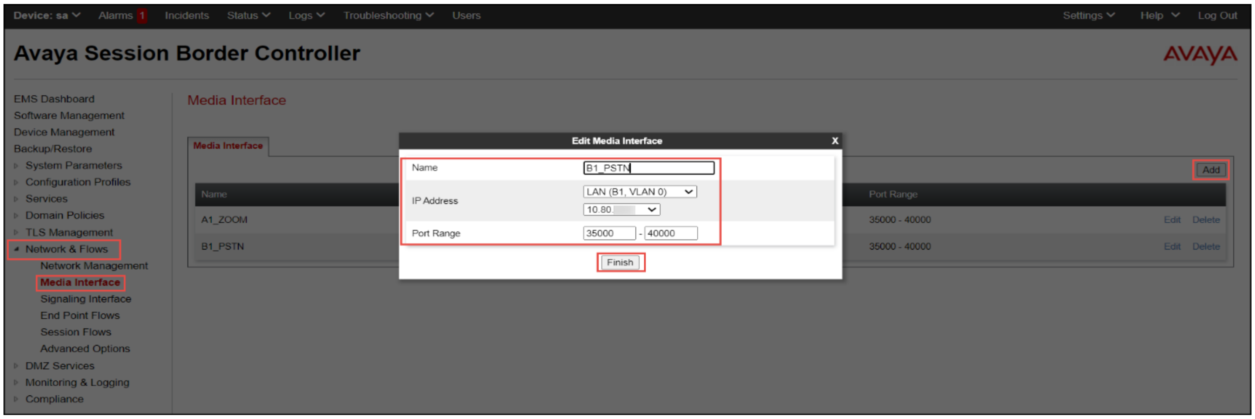
Name	LAN
Default Gateway	10.80.[redacted]
Network Prefix or Subnet Mask	255.255.255.[redacted]
Interface	B1

IP Address	Public IP	Gateway Override	Passthrough	
10.80.[redacted]	Use IP Address	Use Default	□	Delete

Finish

4.3.6 Media Interface

- Navigate to **Network & Flows > Media Interface**. Click **Add**
- Set Name: **B1_PSTN** is given here
- Set IP Address: Select **LAN(B1,VLAN0)** from the drop down and the IP address populates automatically. The IP address for Interface facing PSTN Gateway is **10.XX.XX.XX**
- Set Port Range: **35000-40000**
- Click **Finish**



Name	Port Range		
A1_ZOOM	35000 - 40000	Edit	Delete
B1_PSTN	35000 - 40000	Edit	Delete

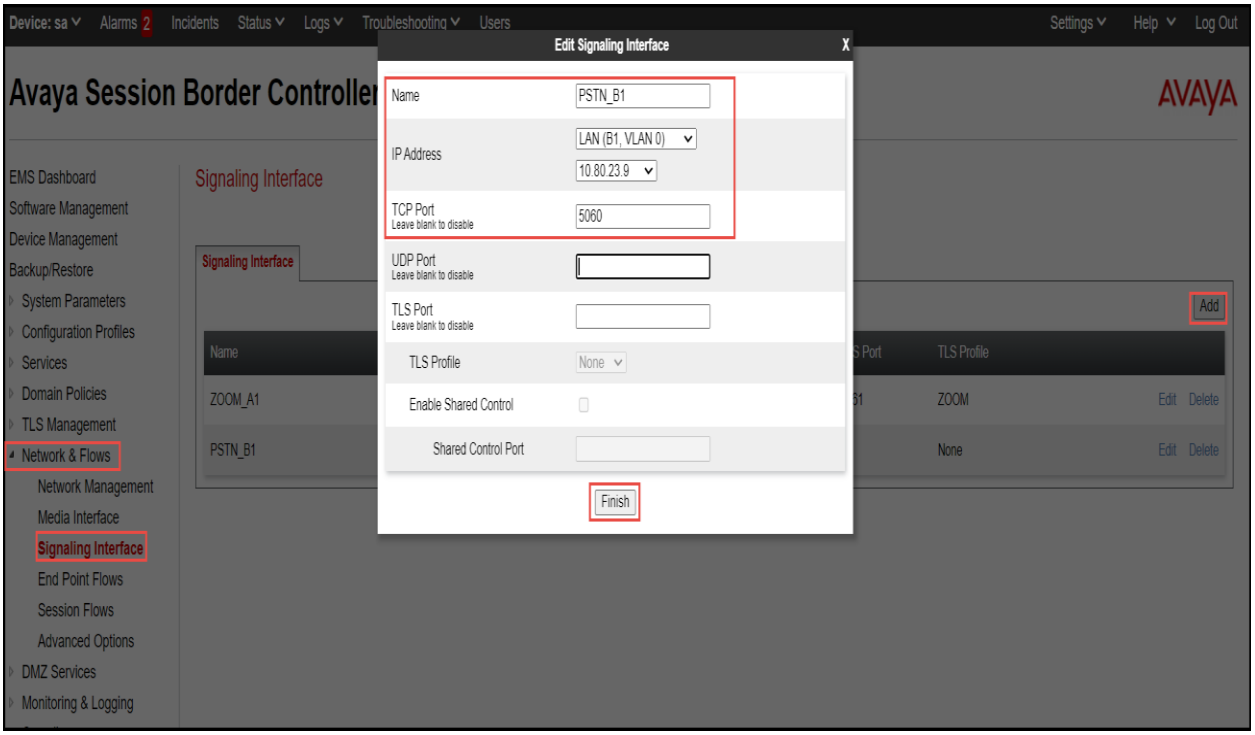
Edit Media Interface

Name	B1_PSTN
IP Address	LAN (B1, VLAN 0) 10.80.[redacted]
Port Range	35000 - 40000

Finish

4.3.7 Signaling Interface

- Navigate to **Network & Flows > Signaling Interface**. Click **Add**, a new Add Signaling Interface window appears
- Set Name: **PSTN_B1** is given for the interface facing **PSTN gateway**
- Set IP Address: Select **LAN(B1, VLAN0)**
- Set TCP Port: **5060**
- Click **Finish**



Edit Signaling Interface

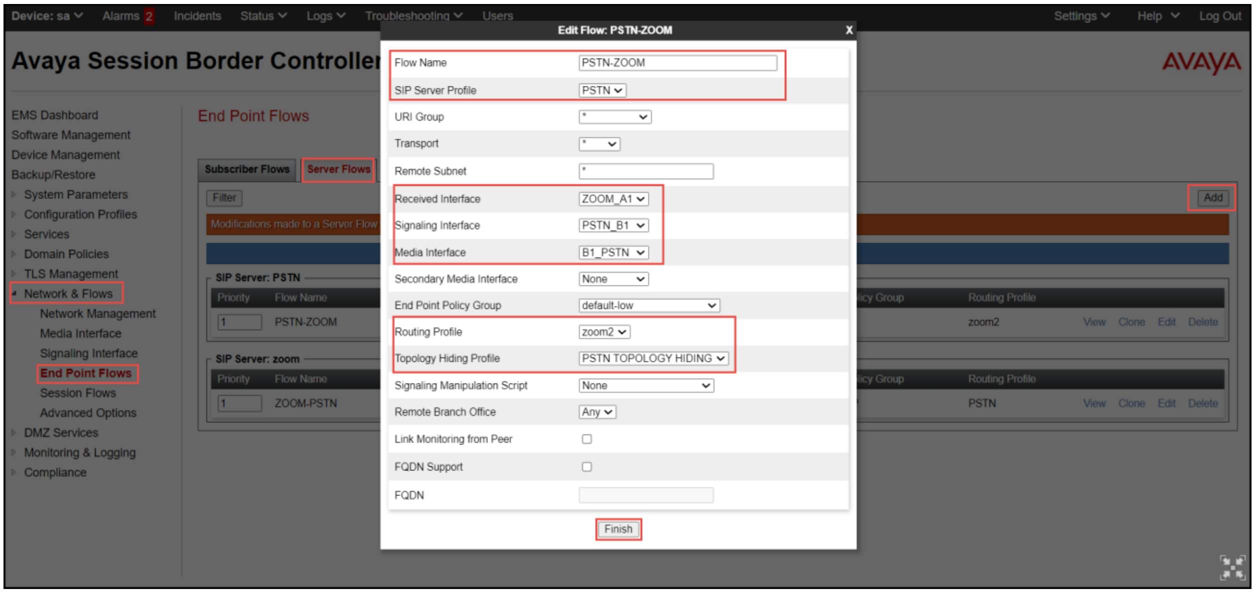
Name	PSTN_B1
IP Address	LAN (B1, VLAN 0) 10.80.23.9
TCP Port Leave blank to disable	5060
UDP Port Leave blank to disable	
TLS Port Leave blank to disable	
TLS Profile	None
Enable Shared Control	□
Shared Control Port	

Finish

Name	S Port	TLS Profile		
ZOOM_A1	61	ZOOM	Edit	Delete
PSTN_B1		None	Edit	Delete

4.3.8 End Point Flow

- Navigate to **Network & Flows** > **End Point Flows** > **Server Flows** and Click **Add**
- Set Flow Name: **PSTN-ZOOM**
- Set SIP Server Profile: **PSTN**
- Received Interface: **ZOOM_A1**
- Signaling Interface: **PSTN_B1**
- Media Interface: **B1_PSTN**
- Routing Profile: **zoom2**
- Topology Hiding Profile: **PSTN TOPOLOGY HIDING**
- Click on **Finish**



Edit Flow: PSTN-ZOOM

Flow Name	PSTN-ZOOM
SIP Server Profile	PSTN
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	ZOOM_A1
Signaling Interface	PSTN_B1
Media Interface	B1_PSTN
Secondary Media Interface	None
End Point Policy Group	default-low
Routing Profile	zoom2
Topology Hiding Profile	PSTN TOPOLOGY HIDING
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	☐
FQDN Support	☐
FQDN	

END OF THE DOCUMENT