

Ribbon SBC Core 5K_7K_SWe R9.0 Interop with Zoom BYOC : Interoperability Guide



Table of Contents

- Interoperable Vendors
- Copyright
- Document Overview
- Non-Goals
- Audience
- Pre-Requisites
- Product and Device Details
- Network Topology Diagram
 - SBC Core Deployment Topology
 - Interoperability Test Lab Topology
- Section A: SBC Core Configuration
 - 1. Network and Connectivity
 - 2. Static Routes
 - Static route towards PSTN
 - Static route towards Zoom
 - 3. TLS Configuration between Ribbon SBC Core and Zoom
 - Generate a CSR with OpenSSL
 - Generate Required Certificates
 - 4. Local Ringback Tone Configuration
 - 5. PSTN Leg Configuration
 - 5.1 Codec Entry
 - 5.2 Packet Service Profile (PSP)
 - 5.3 IP Signaling Profile (IPSP)
 - 5.4 IP Interface Group
 - 5.5 Zone
 - 5.6 SIP Signaling Port
 - 5.7 IP Peer
 - 5.8 SIP Trunk Group
 - 5.9 Routing Label
 - 5.10 Call Routing
 - 6. Zoom Leg Configuration
 - 6.1 Codec Entry
 - 6.2 Packet Service Profile (PSP)
 - 6.3 IP Signaling Profile (IPSP)
 - 6.4 IP Interface Group
 - 6.5 Zone
 - 6.6 SIP Signaling Port
 - 6.7 IP Peer
 - 6.8 SIP Trunk Group
 - 6.9 Routing Label
 - 6.10 Call Routing
- Section B: Configuration for SBC behind NAT
 - SBC behind NAT Topology
 - Additional configuration for SBC behind NAT

- Section C: SBC Core Configuration with External PSX
 - SBC Core configuration
 - Configuration on the PSX
 - Gateway
 - Tone and Announcement Profile
 - Crypto Suite Profile
 - Element Routing Priority
 - Routing Criteria
 - PSTN Leg Configuration
 - IP Signaling Profile (IPSP)
 - Packet Service Profile (PSP)
 - Packet Service Profile ID Group
 - IP Signaling Peer Group
 - Trunk Group
 - Routing Label
 - Zoom Leg Configuration
 - IP Signaling Profile (IPSP)
 - Packet Service Profile (PSP)
 - Packet Service Profile ID Group
 - IP Signaling Peer Group
 - Trunk Group
 - Routing Label
 - Standard Route
- Section D: Zoom Web BYOC Configuration
 - Add External Number
 - Create Zoom Users
 - Supplementary Services Configuration on Zoom
- Supplementary Services & Features Coverage
- Caveats
- Support
- References
- Conclusion

Interoperable Vendors



Copyright

© 2021 Ribbon Communications Operating Company, Inc. © 2021 ECI Telecom Ltd. All rights reserved. The compilation (meaning the collection, arrangement and assembly) of all content on this site is protected by U.S. and international copyright laws and treaty provisions and may not be used, copied, reproduced, modified, published, uploaded, posted, transmitted or distributed in any way, without prior written consent of Ribbon Communications Inc.

The trademarks, logos, service marks, trade names, and trade dress ("look and feel") on this website, including without limitation the RIBBON and RIBBON logo marks, are protected by applicable US and foreign trademark rights and other proprietary rights and are the property of Ribbon Communications Operating Company, Inc. or its affiliates. Any third-party trademarks, logos, service marks, trade names and trade dress may be the property of their respective owners. Any uses of the trademarks, logos, service marks, trade names, and trade dress without the prior written consent of Ribbon Communications Operating Company, Inc., its affiliates, or the third parties that own the proprietary rights, are expressly prohibited.

Document Overview

This document outlines the configuration best practices for the Ribbon SBC Core (SBC 5K, 7K, SWe) 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 local SBC Core are directly connected to the Service Provider of their choice.

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 call flows between Ribbon SBC 5K/7K/SWe and Zoom cloud. Ribbon SBC 5K/7K/SWe is deployed on the customer site to resolve any potential numbering format issue between Zoom and the customer's existing carrier dial plan numbering.

This guide contains the following configuration sections:

- [Section A: SBC Core Configuration](#)
 - Captures general SBC Core configurations for deploying with Zoom BYOC.
- [Section B: Configuration for SBC behind NAT](#)
 - Captures additional SBC configuration performed behind NAT.
- [Section C: Zoom Web BYOC configuration](#)
 - Captures the Zoom BYOC configuration.
 - Test all basic calls, along with the supplementary features like call hold, call transfer, and conference with configurations from Section A and Section B.
 - Configure Advanced supplementary features on Zoom as mentioned in [Supplementary Services Configuration on Zoom](#). These include:
 - Auto Receptionist
 - Call Flip
 - Shared Line Appearance (SLA) or Call Delegation
 - Shared Line Group (SLG)



Note

SBC 5x10, 5400, 7000 and SWe are represented as SBC Core in the following sections.

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 product using graphical user interface (GUI) or command line interface (CLI).

Understanding of the basic concepts of TCP/UDP/TLS, IP/Routing, and SIP/RTP/SRTP 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.

Pre-Requisites

The following aspects are required before proceeding with the interop:

- Ribbon SBC 5K /7K/SWe Core
- Ribbon PSX (if using external PSX instead of ERE (Embedded Routing Engine))
- Public IP Addresses
- Zoom BYOC (Bring Your Own Carrier) Trunk
 - Zoom Go account is required.
 - For more details, visit <https://go.zoom.us/signin>
- TLS Certificates for SBC 5K /7K/SWe Core
 - Please refer to [TLS Configuration between Ribbon SBC Core and Zoom](#)

Product and Device Details

The following equipment and software were used for the sample configuration provided:

Table 1: Requirements

	Equipment	Software Version
Ribbon Communications	Ribbon SBC 5K /7K/SWe Core	V09.00.00R0
	Ribbon PSX	V12.02.02R000
Zoom	Zoom Desktop app	5.0.5 (26213.0602)
	Zoom Mobile app	5.0.5 (26211.0602)
Third-party Equipment	Kapanga Softphone	1.00
	Phonerlite	2.77
	Zoiper	5.3.8

Note

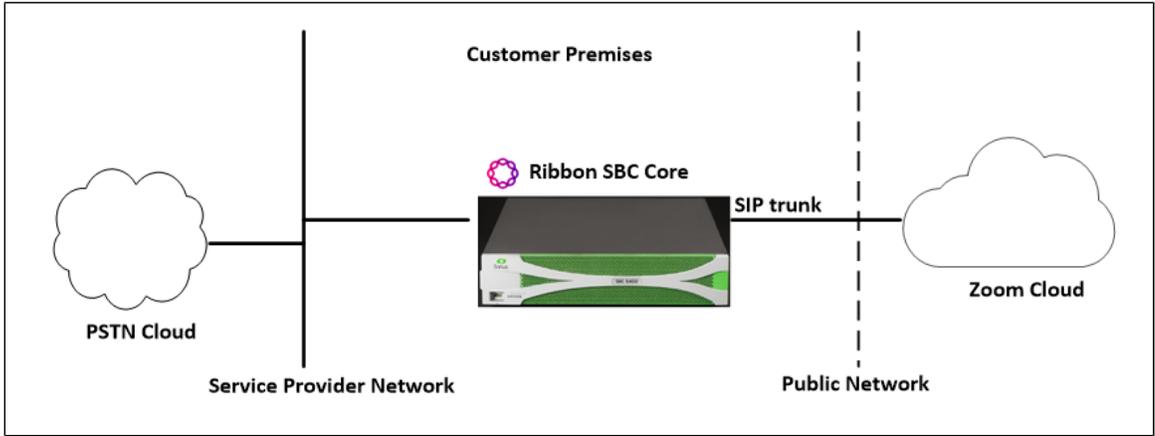
The Ribbon SBC Core portfolio includes SBC 5x10, SBC 5400, SBC 7000 (appliance based), and SBC SWe (virtualized platform). The software version is applicable to Ribbon SBC Core portfolio, and hence, this configuration guide is valid for all these devices.

Network Topology Diagram

This section covers the SBC Core deployment topology and the Interoperability Test Lab Topology.

SBC Core Deployment Topology

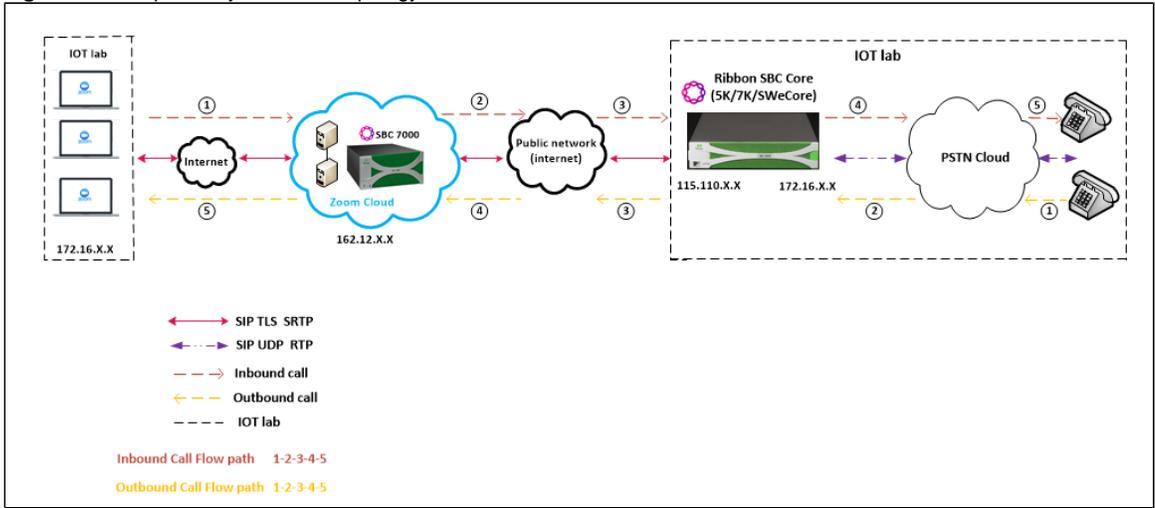
Figure 1: SBC Core Deployment Topology



Interoperability Test Lab Topology

The following lab topology diagram shows connectivity between Zoom and Ribbon SBC Core.

Figure 2: Interoperability Test Lab Topology



Section A: SBC Core Configuration

The following SBC Core configurations are included in this section:

1. [Network and Connectivity](#)
 2. [Static Routes](#)
 3. [TLS Configuration between Ribbon SBC Core and Zoom.](#)
 4. [PSTN Leg Configuration](#)
 5. [Zoom Leg Configuration](#)
- SBC Core can connect to the network as mentioned in [Network and Connectivity](#).
 - Zoom prefers transport as TLS. Establishing a TLS connection between SBC Core and Zoom is covered under [TLS Configuration between Ribbon SBC Core and Zoom](#).
 - SBC Core specific configuration related to PSTN is covered under [PSTN Leg Configuration](#).
 - SBC Core specific configuration related to Zoom is covered under [Zoom Leg Configuration](#).

1. Network and Connectivity

SBC 5400 front and back panel are as shown below:

Figure 3: SBC 5400 Front Panel



Figure 4: SBC 5400 Back Panel



Mgmt - is an RJ45 port and is the management interface of the SBC.

Media 0/1/2/3 depicted as pkt0/pkt1/pkt2/pkt3 are RJ45 ports. Media 0 and Media 1 are used in the current deployment.

2. 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).

Tip

- 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 Voice VLAN or Multi-Switch Edge Devices (MSEs) with Voice VLAN towards SBC Core, static routing configurations are not required.

Add the static route once PSTN Leg and Zoom Leg configurations are done on the SBC.

Static route towards PSTN

```
set addressContext default staticRoute 0.0.0.0 0 10.54.X.X LIF1 PKT0_V4 preference 100
commit
```

Static route towards Zoom

```
set addressContext default staticRoute 162.12.X.X 24 115.110.X.X LIF2 PKT1_V4 preference 100
commit
```

3. TLS Configuration between Ribbon SBC Core and Zoom

Prerequisites:

- For TLS to work on the public side of the network, a trusted CA (Certificate Authority) is needed. In this scenario, GoDaddy is used as a Trusted CA.
- Enable Zoom BYOC trunk with TLS/SRTP.

Generate a CSR with OpenSSL

To create a Certificate Signing Request (CSR) and key file for a Subject Alternative Name (SAN) certificate with multiple subject alternate names, complete the following procedure:

Create an OpenSSL configuration file (text file) on the local computer by editing the fields to the company requirements.

Note 1: In the example used in this article the configuration file is req.conf.

Note 2: req_extensions will put the subject alternative names in a CSR, whereas x509_extensions would be used when creating an actual certificate file.

```
[req]
distinguished_name = req_distinguished_name
req_extensions = v3_req
prompt = no
[req_distinguished_name]
C = US
ST = VA
L = SomeCity
O = MyCompany
OU = MyDivision
CN = www.company.com
[v3_req]
keyUsage = keyEncipherment, dataEncipherment
extendedKeyUsage = serverAuth
subjectAltName = @alt_names
[alt_names]
DNS.1 = www.company.com
DNS.2 = company.com
DNS.3 = www.company.net
DNS.4 = company.net
```

Make sure there are no whitespaces at the end of the lines.

#Run the following commands to create the Certificate Signing Request (CSR) and a new Key file:

```
openssl req -new -out company_san.csr -newkey rsa:2048 -nodes -sha256 -keyout company_san.key.temp -config req.conf
```

#Run the following command to verify the Certificate Signing Request:

```
openssl req -text -noout -verify -in company_san.csr
```

After receiving the CSR with above information, provide it to CA (Certificate Authority). You will then receive the proper CA signed certificate in .crt format that is convertible into other formats using openssl.

By default, you should receive two or more certificates from CA (depending upon your CA). One is the SBC certificate, and other is CA's root and intermediate certificate.

Upload the certificates to the SBC at /opt/sonus/external and convert them into SBC-readable format, i.e. SBC certificate is in .pem or .p12 format and root certificate is in .cer or .der.

#Converting .crt to .pem USING OPENSLL for SBC certificate.

```
openssl x509 -in sbc_cert.crt -out sbc_cert.der -outform DER
```

```
openssl x509 -in sbc_cert.der -inform DER -out sbc_cert.pem -outform PEM
```

#After generating sbc_cert.pem file, convert it to .p12 format using below command and the location of the certificate key.

```
openssl pkcs12 -export -out sbc1_cert.p12 -in sbc_cert.pem -inkey /opt/sonus/company_san.key.temp
```

#CONVERTING CRT to CER USING OPENSLL for CA's root and intermediate certificate.

```
openssl x509 -in root_cert.crt -out root_cert.cer -outform DER
```

After converting all these certificates upload them on SBC at /opt/sonus/external location.

Generate Required Certificates

```
#Import Public CA Root Certificate into database.
set system security pki certificate CA_ROOT_CERT type remote fileName root_cert.cer state enabled

#Import Public CA Certified SBC Server Certificate into database.
set system security pki certificate SBC_CERT filename sbcl_cert.p12 passphrase <Password defined during CSR
generation> state enabled type local
```

TLS Profile

A TLS Profile is required for the TLS handshake between SBC Core and Zoom. This profile defines cipher suites supported by SBC Core. Create the TLS profile as mentioned below:

```
set profiles security tlsProfile TLS_PROF clientCertName SBC_CERT serverCertName SBC_CERT cipherSuite1
tls_ecdhe_rsa_with_aes_256_gcm_sha384 cipherSuite2 tls_ecdhe_rsa_with_aes_128_gcm_sha256 authClient true allowedRoles
clientandserver acceptableCertValidationErrors invalidPurpose
set profiles security tlsProfile TLS_PROF v1_1 enable
set profiles security tlsProfile TLS_PROF v1_0 disable
set profiles security tlsProfile TLS_PROF v1_2 enable
commit
```

Attach the TLS Profile to the SIP Signaling Port that will be created later in Zoom Leg Configuration.

```
set addressContext default zone ZOOM sipSigPort 7 state disabled mode outOfService
commit
set addressContext default zone ZOOM sipSigPort 7 tlsProfileName TLS_PROF
commit
set addressContext default zone ZOOM sipSigPort 7 state enabled mode inService
commit
```

4. Local Ringback Tone Configuration

This section contains the general SBC configurations.

DSP Resource Allocation

This configuration only applies if the SBC has been deployed with (hardware) DSP resources. If it has not, executing this configuration step has no negative impact. Do not attempt transcoding, so that the lack of compression resources will not impact the overall SBC configuration in this document.

```
set system mediaProfile compression 75 tone 25
commit
```



This configuration is not required for SBC SWe 7.2 release onwards.

Local Ringback Tone (LRBT) Profile

1. Create a Local Ringback Tone (LRBT) profile that is attached to both PSTN and Zoom leg.
2. Enable Dynamic LRBT.

```
set profiles media toneAndAnnouncementProfile LRBT_PROF
set profiles media toneAndAnnouncementProfile LRBT_PROF localRingBackTone signalingTonePackageState enable
set profiles media toneAndAnnouncementProfile LRBT_PROF localRingBackTone precedence lower
set profiles media toneAndAnnouncementProfile LRBT_PROF localRingBackTone makeInbandToneAvailable enable
set profiles media toneAndAnnouncementProfile LRBT_PROF localRingBackTone flags useThisLrbtForEgress enable
set profiles media toneAndAnnouncementProfile LRBT_PROF localRingBackTone flags useThisLrbtForIngress enable
set profiles media toneAndAnnouncementProfile LRBT_PROF localRingBackTone flags dynamicLRBT enable
commit
```

5. PSTN Leg Configuration

Create profiles with a specific set of characteristics corresponding to PSTN. This includes configuration of the following entities on PSTN leg:

1. [Codec Entry](#)
2. [Packet Service Profile](#)
3. [IP Signaling Profile](#)
4. [IP Interface Group](#)
5. [Zone](#)
6. [SIP Signaling Port](#)
7. [IP Peer](#)
8. [SIP Trunk Group](#)
9. [Routing Label](#)
10. [Call Routing](#)

5.1 Codec Entry

Codec entry allows you to specify the codec used for the call. Create the codec entry for G711Ulaw codec with packet size 20 and rfc2833 method for dtmf.

```
set profiles media codecEntry G711ULAW codec g711
set profiles media codecEntry G711ULAW law ULaw
set profiles media codecEntry G711ULAW packetSize 20
set profiles media codecEntry G711ULAW dtmf relay rfc2833
commit
```

5.2 Packet Service Profile (PSP)

Create a Packet Service Profile (PSP) for the PSTN leg. The PSP is attached to sipTrunkGroup created later in this section.

```
set profiles media packetServiceProfile PSTN_PSP codec codecEntry1 G711ULAW
set profiles media packetServiceProfile PSTN_PSP rtcpOptions rtcp enable
commit
```

5.3 IP Signaling Profile (IPSP)

Create an IP Signaling Profile with appropriate signaling flags towards PSTN.

```
set profiles signaling ipSignalingProfile PSTN_IPSP
set profiles signaling ipSignalingProfile PSTN_IPSP egressIpAttributes flags disable2806Compliance enable
commit
```

5.4 IP Interface Group

Create an IP interface group.

 Replace "x.x.x.x" with the SBC's packet interface (pkt) IP address towards PSTN (example pkt0 IP), and "Y" with its prefix length. Provide ceName used during an SBC deployment.

Here the ceName is "ZOOM1".

```
set addressContext default ipInterfaceGroup LIF1 ipInterface PKT0_V4 ceName ZOOM1 portName pkt0
set addressContext default ipInterfaceGroup LIF1 ipInterface PKT0_V4 ipAddress x.x.x.x prefix Y
set addressContext default ipInterfaceGroup LIF1 ipInterface PKT0_V4 mode inService state enabled
commit
```

5.5 Zone

Create Zone towards PSTN and specify the id of the zone.

 This Zone groups the set of objects used for the communication towards PSTN.

```
set addressContext default zone PSTN id 2
commit
```

5.6 SIP Signaling Port

Set the SIP Signaling port, which is a logical address used to send and receive SIP call signaling packets and is permanently bound to a specific zone.

 Replace "x.x.x.x" with SIP Signaling Port IP of SBC towards PSTN.

```
set addressContext default zone PSTN sipSigPort 3 ipInterfaceGroupName LIF1
set addressContext default zone PSTN sipSigPort 3 ipAddressV4 x.x.x.x
set addressContext default zone PSTN sipSigPort 3 portNumber 5060
set addressContext default zone PSTN sipSigPort 3 transportProtocolsAllowed sip-udp
set addressContext default zone PSTN sipSigPort 3 mode inService
set addressContext default zone PSTN sipSigPort 3 state enabled
commit
```

5.7 IP Peer

Create an IP Peer with the signaling IP address of the PSTN (Service Provider) and assign it to the PSTN Zone.

 Replace "x.x.x.x" with the PSTN IP.

```
set addressContext default zone PSTN ipPeer PSTN_IPP ipAddress x.x.x.x
set addressContext default zone PSTN ipPeer PSTN_IPP ipPort 5060
commit
```

5.8 SIP Trunk Group

Create a SIP Trunk Group towards the PSTN and assign corresponding profiles like LRBT, PSP, IPSP created in earlier steps.

 You must configure Trunk Group names using capital letters.

```
set addressContext default zone PSTN sipTrunkGroup PSTN_TG media mediaIpInterfaceGroupName LIF1
set addressContext default zone PSTN sipTrunkGroup PSTN_TG mode inService state enabled
commit

set addressContext default zone PSTN sipTrunkGroup PSTN_TG policy signaling ipSignalingProfile PSTN_IPSP
set addressContext default zone PSTN sipTrunkGroup PSTN_TG policy media packetServiceProfile PSTN_PSP
set addressContext default zone PSTN sipTrunkGroup PSTN_TG policy media toneAndAnnouncementProfile LRBT_PROF
set addressContext default zone PSTN sipTrunkGroup PSTN_TG ingressIpPrefix 0.0.0.0 0
commit
```

5.9 Routing Label

Create a Routing Label with a single Routing Label Route to bind the PSTN Trunk Group with the PSTN IP Peer.

```
set global callRouting routingLabel PSTN_RL routingLabelRoute 1 trunkGroup PSTN_TG
set global callRouting routingLabel PSTN_RL routingLabelRoute 1 ipPeer PSTN_IPP
set global callRouting routingLabel PSTN_RL routingLabelRoute 1 inService inService
commit
```

5.10 Call Routing

This entry is used to route all the calls coming from PSTN towards ZOOM endpoints.

 Provide ceName used during an SBC deployment. "ZOOM1" is the ceName.

```
set global callRouting route trunkGroup PSTN_TG ZOOM1 standard Sonus_NULL 1 all all ALL none Sonus_NULL
routingLabel ZOOM_RL
commit
```

6. Zoom Leg Configuration

Create profiles with a specific set of characteristics corresponding to Zoom. This includes configuration of the following entities on Zoom leg:

1. [Codec Entry](#)
2. [Packet Service Profile](#)
3. [IP Signaling Profile](#)
4. [IP Interface Group](#)
5. [Zone](#)
6. [SIP Signaling Port](#)
7. [IP Peer](#)
8. [SIP Trunk Group](#)
9. [Routing Label](#)
10. [Call Routing](#)

6.1 Codec Entry

Codec entry allows you to specify the codec used for the call. Create the codec entry for G711Ulaw codec with packet size 20 and rfc2833 method for dtmf.

```
set profiles media codecEntry G711_Zoom codec g711
set profiles media codecEntry G711_Zoom law ULaw
set profiles media codecEntry G711_Zoom packetSize 20
set profiles media codecEntry G711_Zoom dtmf relay rfc2833
commit
```

6.2 Packet Service Profile (PSP)

Create a Packet Service Profile (PSP) for the Zoom leg. The PSP is attached to the sipTrunkGroup that is created later in this section.

Since there is an SRTP between the SBC Core and Zoom, you must create a crypto suite profile.

```
set profiles security cryptoSuiteProfile CRYPT_PROF entry 1 cryptoSuite AES-CM-128-HMAC-SHA1-80
```

The Crypto Suite profile is attached to the ZOOM_PSP.

```
set profiles media packetServiceProfile ZOOM_PSP codec codecEntry1 G711_Zoom
set profiles media packetServiceProfile ZOOM_PSP rtcpOptions rtcp enable
set profiles media packetServiceProfile ZOOM_PSP secureRtpRtcp cryptoSuiteProfile CRYPT_PROF
set profiles media packetServiceProfile ZOOM_PSP secureRtpRtcp flags allowFallback enable
set profiles media packetServiceProfile ZOOM_PSP secureRtpRtcp flags enableSrtp enable
commit
```

6.3 IP Signaling Profile (IPSP)

Create an IP Signaling Profile with appropriate signaling flags towards Zoom.

 The SBC Core to Zoom transport type is TLS and therefore enables the same transport type in ZOOM_IPSP.

```
set profiles signaling ipSignalingProfile ZOOM_IPSP
set profiles signaling ipSignalingProfile ZOOM_IPSP egressIpAttributes flags disable2806Compliance enable
set profiles signaling ipSignalingProfile ZOOM_IPSP egressIpAttributes numberGlobalizationProfile DEFAULT_IP
set profiles signaling ipSignalingProfile ZOOM_IPSP egressIpAttributes transport type1 tlsOverTcp
commit
```

6.4 IP Interface Group

Create an IP interface group.

 Replace "x.x.x.x" with the SBC's packet interface (pkt) IP address towards ZOOM (example pkt1 IP), and "Y" with its prefix length. Provide the ceName used during an SBC deployment.

Here the ceName is "ZOOM1".

```
set addressContext default ipInterfaceGroup LIF2 ipInterface PKT1_V4 ceName ZOOM1 portName pkt1
set addressContext default ipInterfaceGroup LIF2 ipInterface PKT1_V4 ipAddress x.x.x.x prefix Y
set addressContext default ipInterfaceGroup LIF2 ipInterface PKT1_V4 mode inService state enabled
commit
```

6.5 Zone

Create a Zone towards Zoom and specify the id of the zone.

 This Zone groups the set of objects used for communication towards Zoom.

```
set addressContext default zone ZOOM id 6
commit
```

6.6 SIP Signaling Port

Set the SIP Signaling port, which is a logical address used to send and receive SIP call signaling packets and is permanently bound to a specific zone.

 Replace "x.x.x.x" with the SIP Signaling Port IP address of the SBC towards Zoom.

```
set addressContext default zone ZOOM sipSigPort 7 ipInterfaceGroupName LIF2
set addressContext default zone ZOOM sipSigPort 7 ipAddressV4 x.x.x.x
set addressContext default zone ZOOM sipSigPort 7 portNumber 5060
set addressContext default zone ZOOM sipSigPort 7 tlsProfileName TLS_PROF
set addressContext default zone ZOOM sipSigPort 7 transportProtocolsAllowed sip-tls-tcp
set addressContext default zone ZOOM sipSigPort 7 mode inService
set addressContext default zone ZOOM sipSigPort 7 state enabled
commit
```



You created the TLS profile in [TLS Profile](#).



There are a few areas that result in a TLS negotiation issue. One area involves assigning the incorrect port. Ensure the following are accomplished:

- Zoom listens on port number 5061 (default setting).
- Configure port number 5060 on Zoom IP-Peer since Ribbon SBC Core increments the port by 1 when the transport protocol is TLS.

6.7 IP Peer

Create an IP Peer with the signaling IP address of ZOOM and assign it to ZOOM Zone.



Replace "x.x.x.x" with the Zoom SIP signaling IP.

```
set addressContext default zone ZOOM ipPeer ZOOM_IPP ipAddress x.x.x.x
set addressContext default zone ZOOM ipPeer ZOOM_IPP ipPort 5060
commit
```

Path Check Profile

Create a path check profile that attaches to the Zoom side.

```
set profiles services pathCheckProfile ZOOM_OPTIONS protocol sipOptions sendInterval 20 replyTimeoutCount 1
recoveryCount 1
set profiles services pathCheckProfile ZOOM_OPTIONS transportPreference preference1 tls-tcp
commit
```

6.8 SIP Trunk Group

Create a SIP Trunk Group towards ZOOM and assign corresponding profiles like LRBT, PSP, IPSP that were created in earlier steps.



You must configure Trunk Group names using capital letters.

```
set addressContext default zone ZOOM sipTrunkGroup ZOOM_TG media mediaIpInterfaceGroupName LIF2
set addressContext default zone ZOOM sipTrunkGroup ZOOM_TG mode inService state enabled
commit

set addressContext default zone ZOOM sipTrunkGroup ZOOM_TG policy signaling ipSignalingProfile ZOOM_IPSP
set addressContext default zone ZOOM sipTrunkGroup ZOOM_TG policy media packetServiceProfile ZOOM_PSP
set addressContext default zone ZOOM sipTrunkGroup ZOOM_TG policy media toneAndAnnouncementProfile LRBT_PROF
set addressContext default zone ZOOM sipTrunkGroup ZOOM_TG ingressIpPrefix 0.0.0.0 0
commit
```

6.9 Routing Label

Create a Routing Label with a single Routing Label Route to bind the ZOOM Trunk Group with the ZOOM IP Peer.

```
set global callRouting routingLabel ZOOM_RL routingLabelRoute 1 trunkGroup ZOOM_TG
set global callRouting routingLabel ZOOM_RL routingLabelRoute 1 ipPeer ZOOM_IPP
set global callRouting routingLabel ZOOM_RL routingLabelRoute 1 inService inService
commit
```

6.10 Call Routing

This entry is used to route all the calls coming from Zoom towards PSTN endpoints.

 Provide the ceName used during an SBC deployment. "ZOOM1" is the ceName.

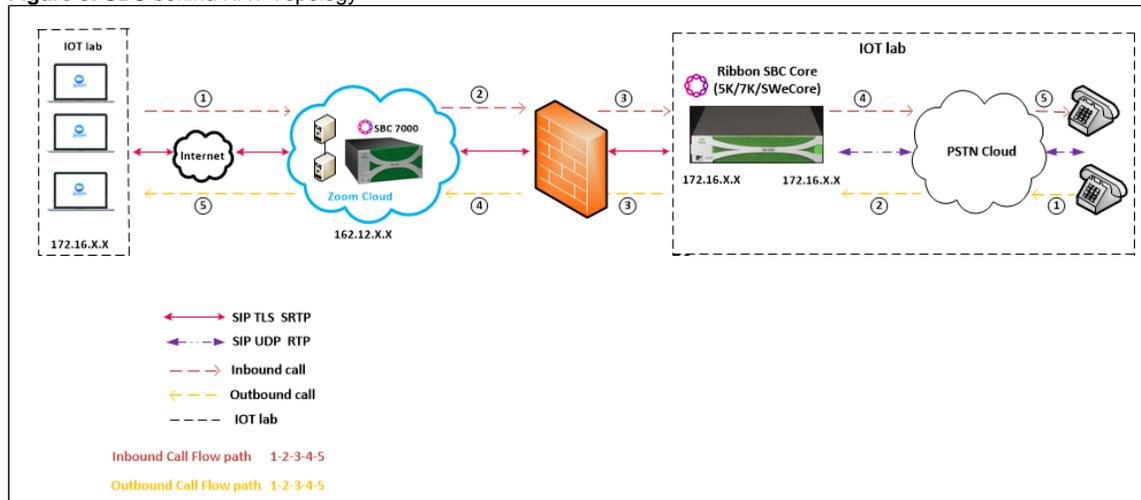
```
set global callRouting route trunkGroup ZOOM_TG ZOOM1 standard Sonus_NULL 1 all all ALL none Sonus_NULL
routingLabel PSTN_RL
commit
```

Section B: Configuration for SBC behind NAT

Telecom operators do not expose the WAN side of the SBC directly to the public network. The SBC is deployed in the DMZ behind a NAT'ed device having WAN interface configured with a private IP. To achieve this, certain SIP Message Manipulation (SMM) rules are applied in the SBC for converting Private IP to Public IP.

SBC behind NAT Topology

Figure 5: SBC behind NAT Topology



Additional configuration for SBC behind NAT

SIP Trunk Group towards Zoom

Add the following additional configuration to the SIP Trunk Group towards the Zoom leg.

```
set addressContext default zone ZOOM sipTrunkGroup ZOOM_TG services natTraversal signalingNat enabled
set addressContext default zone ZOOM sipTrunkGroup ZOOM_TG services natTraversal mediaNat enabled
commit
```

Outbound Profile

An SMM rule "HeaderModification" is used to replace the Private IP with the Public IP.

 Replace the <Private_IP> and <Public_IP> with actual IP's.

```
set profiles signaling sipAdaptorProfile HeaderModifications state enabled
set profiles signaling sipAdaptorProfile HeaderModifications profileType messageManipulation
set profiles signaling sipAdaptorProfile HeaderModifications rule 1 applyMatchHeader one
set profiles signaling sipAdaptorProfile HeaderModifications rule 1 criterion 1 type message
set profiles signaling sipAdaptorProfile HeaderModifications rule 1 criterion 1 message
set profiles signaling sipAdaptorProfile HeaderModifications rule 1 criterion 1 message messageTypes all
set profiles signaling sipAdaptorProfile HeaderModifications rule 1 action 1 type messageBody
set profiles signaling sipAdaptorProfile HeaderModifications rule 1 action 1 operation regsub
set profiles signaling sipAdaptorProfile HeaderModifications rule 1 action 1 from
set profiles signaling sipAdaptorProfile HeaderModifications rule 1 action 1 from type value
set profiles signaling sipAdaptorProfile HeaderModifications rule 1 action 1 from value <Public_IP>
set profiles signaling sipAdaptorProfile HeaderModifications rule 1 action 1 to
set profiles signaling sipAdaptorProfile HeaderModifications rule 1 action 1 to type messageBody
set profiles signaling sipAdaptorProfile HeaderModifications rule 1 action 1 to messageBodyValue all
set profiles signaling sipAdaptorProfile HeaderModifications rule 1 action 1 regexp
set profiles signaling sipAdaptorProfile HeaderModifications rule 1 action 1 regexp string <Private_IP>
set profiles signaling sipAdaptorProfile HeaderModifications rule 1 action 1 regexp matchInstance all
set profiles signaling sipAdaptorProfile HeaderModifications rule 2 applyMatchHeader one
set profiles signaling sipAdaptorProfile HeaderModifications rule 2 criterion 1 type message
set profiles signaling sipAdaptorProfile HeaderModifications rule 2 criterion 1 message
set profiles signaling sipAdaptorProfile HeaderModifications rule 2 criterion 1 message messageTypes all
set profiles signaling sipAdaptorProfile HeaderModifications rule 2 criterion 2 type header
set profiles signaling sipAdaptorProfile HeaderModifications rule 2 criterion 2 header
set profiles signaling sipAdaptorProfile HeaderModifications rule 2 criterion 2 header name Contact
set profiles signaling sipAdaptorProfile HeaderModifications rule 2 criterion 2 header condition exist
set profiles signaling sipAdaptorProfile HeaderModifications rule 2 criterion 2 header hdrInstance all
set profiles signaling sipAdaptorProfile HeaderModifications rule 2 action 1 type header
set profiles signaling sipAdaptorProfile HeaderModifications rule 2 action 1 operation regsub
set profiles signaling sipAdaptorProfile HeaderModifications rule 2 action 1 headerInfo fieldValue
set profiles signaling sipAdaptorProfile HeaderModifications rule 2 action 1 from
set profiles signaling sipAdaptorProfile HeaderModifications rule 2 action 1 from type value
set profiles signaling sipAdaptorProfile HeaderModifications rule 2 action 1 from value <Public_IP>
set profiles signaling sipAdaptorProfile HeaderModifications rule 2 action 1 to
set profiles signaling sipAdaptorProfile HeaderModifications rule 2 action 1 to type header
set profiles signaling sipAdaptorProfile HeaderModifications rule 2 action 1 to value Contact
set profiles signaling sipAdaptorProfile HeaderModifications rule 2 action 1 regexp
set profiles signaling sipAdaptorProfile HeaderModifications rule 2 action 1 regexp string <Private_IP>
set profiles signaling sipAdaptorProfile HeaderModifications rule 2 action 1 regexp matchInstance all
```

Attach the SMM rule to the OutputAdapter Profile of ZOOM_TG

```
set addressContext default zone ZOOM sipTrunkGroup ZOOM_TG signaling messageManipulation outputAdapterProfile
HeaderModifications
commit
```

Section C: SBC Core Configuration with External PSX

SBC Core configuration

The following SBC configurations remain the same as mentioned in [Section A: SBC Core Configuration](#).

1. [Network and Connectivity](#)
2. [Static Routes](#)
3. [TLS Configuration between Ribbon SBC Core and Zoom](#)
4. [Local Ringback Tone Configuration](#) – Configure only the [DSP Resource Allocation](#) on SBC Core. [Local Ringback Tone \(LRBT\) Profile](#) is configured in the external PSX, as shown later.
5. [PSTN Leg Configuration](#) – Configure the [IP Interface Group](#), [Zone](#), [SIP Signaling Port](#) and [SIP Trunk Group](#) as mentioned in this section.
6. [Zoom Leg Configuration](#) – Configure the [IP Interface Group](#), [Zone](#), [SIP Signaling Port](#) and [SIP Trunk Group](#) as mentioned in this section.

Enable Remote PSX Server

By default, the SBC Core is enabled with a local PSX server. You must disable the local PSX to enable the remote PSX.

Command to disable the local PSX server.

```
set system policyServer localServer PSX_LOCAL_SERVER state disabled mode outOfService
```

Command to enable the remote PSX server.

```
set system policyServer remoteServer RBBNPSX ipAddress 172.16.X.X state enabled mode active
```

 "RBBNPSX" is the name of the remote PSX server. Provide the valid IP of the remote PSX server.

Configuration on the PSX

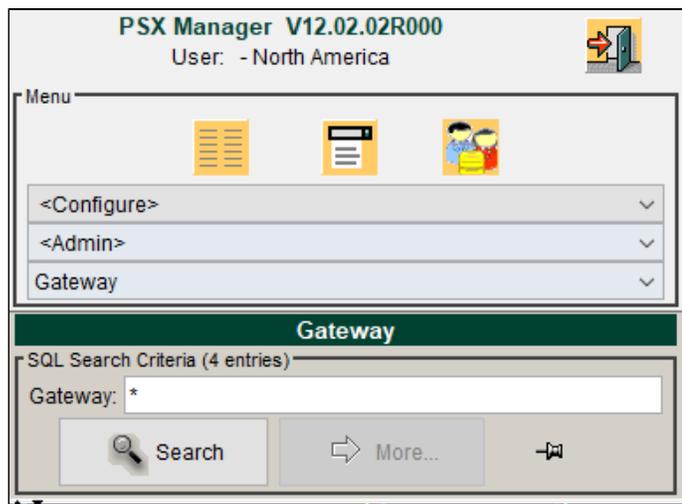
This section provides the configuration aspects required on the PSX side.

 The sequence of steps covering various snapshots & information provided in the snapshots for PSX configuration must be meticulously followed.

Gateway

Configure a gateway with SBC name and it's management IP address.

Figure 6: Gateway Creation



Host: 172.16.100.216 @ 4330
Master (SWe) - V12.02.02R000

View: Gateway | Close All | Perspective: Full View

GATEWAY: ZOOM | LRNS

Switch: ZOOM

Gateway Group: DEFAULT

Cluster Profile: <None>

Default Trunk Group: SIP

Charge Band Profile: <None>

Traffic Control Escape Profile: <None>

Mobile Switch ID: 1 None

Signaling Gateway Group: <None>

Enum Authority Profile: <None>

Address Reachability Service Profile: <None>

SMM Profile Group: <None>

Peer Throttling Profile: <None>

P-Origination-ID:

Flags

CAMEL Services Supported Route CAMEL Subscription Calls

CDP Gateway Traffic Management

MTRR Supported Logical SBC

Display

Allow Mixed Characters in Gateway Name

Flags

CAMEL Services Supported Route CAMEL Subscription Calls

CDP Gateway Traffic Management

MTRR Supported Logical SBC

Display

Allow Mixed Characters in Gateway Name

H.323 Control

Prune Routes

Network

IPv4 Address: 10 . 54 . [red] . [red] Port Number: 2569

IPv6 Address: 0 : 0 : 0 : 0 : 0 : 0 : 0 : 0

Prefer IPv4 Prefer IPv6

H.323 IPv4 Address: 0 . 0 . 0 . 0 H.323 Port Number: 1720

H323 IPv6 Address: 0 : 0 : 0 : 0 : 0 : 0 : 0 : 0

Set As Default H.323 Gateway For This IP Address

Prefer IPv4 Prefer IPv6

SIP IPv4 Address: 0 . 0 . 0 . 0 SIP Port Number: 5060

SIP IPv6 Address: 0 : 0 : 0 : 0 : 0 : 0 : 0 : 0

Set As Default SIP Gateway For This IP Address

Save | Cancel | Delete

Tone and Announcement Profile

Configure the Tone and Announcement Profile as shown below:

Figure 7: Tone And Announcement Profile

Tone And Announcement Profile: ZOOM_LRBT

Local Ring Back Tone

Signaling Tone Package: 1 - DEFAULT

Precedence: Lower Higher

Make Inband Tone Available

Flags

Force Local Ring Back Tone Dynamic Local Ring Back Tone

Use This Local Ring Back Tone For Egress Use This Local Ring Back Tone For Ingress

Announcement Based Tones 180WithOrWithOutSdp

EarlyMediaMethod: None

Tone And Announcement Profile

Announcement Package: 1 - DEFAULT

Signaling Tone Package: 1 - DEFAULT

Override

Tone Generation Criteria

Tone Generation Criteria: <None>

Crypto Suite Profile

Select the Crypto Suite as "AES CM 128 HMAC SHA1 80".

Figure 8: Crypto Suite Profile

Crypto Suite Profile: ZOOM_CRYPT

Description: Secure Crypto Suite Profile for Zoom

Crypto Suites

Sequence: 1

Crypto Suite: AES CM 128 HMAC SHA1 80

Session Parameter Flags

Unauthenticated SRTP Unencrypted SRTP

Unencrypted SRTCP

Add/Update

Sequence	Crypto Suite
1	AES CM 128 HMAC SHA1 80

Element Routing Priority

Assign the highest priority to the Entity Type Trunk Group for all the required Call Types.

Figure 9: Element RP

Element Routing Priority: ZOOM_ERP

Call Property

Call Type: 1+
 Priority: 1
 Network: All
 Toll Indication: <All>

Entity Type: Trunk Group
 Priority: 1

Add Update

Call Type	Call Priority	Network	Toll Indication	Entity Type	Priority
Private	1	All	<All>	<None>	1
0+	1	All	<All>	<None>	1
0-	1	All	<All>	<None>	1
1+	1	All	<All>	Trunk Group	1
1+	2	All	<All>	<None>	2
IDDD	1	All	<All>	<None>	1
0+ IDDD	1	All	<All>	<None>	1
00	1	All	<All>	<None>	1
IP VPN Service	1	All	<All>	<None>	1
Test	1	All	<All>	<None>	1
Transit	1	All	<All>	<None>	1
Other Carrier Chosen	1	All	<All>	<None>	1
Carrier Cut Through	1	All	<All>	<None>	1
User Name	1	All	<All>	<None>	1
Mobile	1	All	<All>	<None>	1

Delete

Back To Softlink Save Cancel Delete

Routing Criteria

Use the Routing criteria "DEFAULT_IP" as shown below. The configuration is as follows:

Figure 10: Routing C

Routing Criteria: DEFAULT_IP

Call Property

Call Type: 1+
 Priority: 1
 Network: All
 Toll Indication: <All>

Use Destination Use Partition

Add Update

Call Type	Call Priority	Network	Toll Indication	Use Destination	Use Partition
Private	1	All	<All>	Enabled	Enabled
0+	1	All	<All>	Enabled	Enabled
0-	1	All	<All>	Enabled	Enabled
1+	1	All	<All>	Enabled	Enabled
IDDD	1	All	<All>	Enabled	Enabled
0+ IDDD	1	All	<All>	Enabled	Enabled
00	1	All	<All>	Enabled	Enabled
IP VPN Service	1	All	<All>	Enabled	Enabled
Test	1	All	<All>	Enabled	Enabled
Transit	1	All	<All>	Enabled	Enabled
Other Carrier Chosen	1	All	<All>	Enabled	Enabled
Carrier Cut Through	1	All	<All>	Enabled	Enabled
User Name	1	All	<All>	Enabled	Enabled
Mobile	1	All	<All>	Enabled	Enabled

Delete

Back To Softlink Save Cancel Delete

PSTN Leg Configuration

IP Signaling Profile (IPSP)

Create an IP Signaling Profile with the appropriate signaling flags towards PSTN.

Figure 11: IP Signaling Profile

IP SIGNALING PROFILE: PSTN_IPSP

Common IP Attributes - Communicating With The Peer Regardless Of Call Direction

<input type="checkbox"/> Accept Alert Info	<input type="checkbox"/> No Content Disposition
<input type="checkbox"/> Add P-Charging Function Addr	<input type="checkbox"/> No Port Number 5060
<input type="checkbox"/> Add Path/Service Route Per TG	<input type="checkbox"/> No Userinfo In Contact Header
<input type="checkbox"/> Audio Codec Change through Empty TCS	<input type="checkbox"/> Only Selected Codec In Session Refresh
<input type="checkbox"/> Call Hold Interworking	<input type="checkbox"/> Override Relay For Non SIP Egress Leg
<input type="checkbox"/> Calling Party Type Number If Present	<input type="checkbox"/> P-Called-Party-Id-Support
<input type="checkbox"/> Clearmode For Data Calls	<input type="checkbox"/> P-ChgMsg-Info
<input type="checkbox"/> Create P-Charging-Vector	<input type="checkbox"/> Relay Data Path Mode Changes To The Other Leg
<input type="checkbox"/> Create P-Visited-Network Id	<input type="checkbox"/> Reject REFER
<input type="checkbox"/> Create Path Header	<input type="checkbox"/> Replace Host On Via Header
<input type="checkbox"/> Create Service-Route Header	<input type="checkbox"/> Reject REFER With IP
<input type="checkbox"/> Customized Session Timer Behavior	<input type="checkbox"/> Reject REFER With TN
<input type="checkbox"/> Disable Also Header	<input type="checkbox"/> ReQuery PSX on REGISTER Refresh
<input type="checkbox"/> Disable Constrained Capacities	<input type="checkbox"/> Restrict History Info Header
<input type="checkbox"/> Disable Host Translation	<input type="checkbox"/> Route Using Received FQDN
<input type="checkbox"/> Disable Media Lock Down	<input type="checkbox"/> SDP O-line Only Compares
<input type="checkbox"/> Disable Refer-To URI Parameters	<input type="checkbox"/> Send All Allowed Codecs For Late Media Invite Or Re-Invite
<input type="checkbox"/> Discard Received Reason Header	<input type="checkbox"/> Send Direct Media Info In SDP Attribute
<input type="checkbox"/> Do Not Include SS Attribute In Re-INVITE	<input type="checkbox"/> Send Empty TCS

<input type="checkbox"/> Don't Send REFER With TN	<input type="checkbox"/> Send PTIME In SDP
<input type="checkbox"/> End To End BYE	<input type="checkbox"/> Send RTCP Port In SDP
<input type="checkbox"/> End To End RE-INVITE	<input type="checkbox"/> Session Timer Refresh Update
<input type="checkbox"/> End To End UPDATE	<input type="checkbox"/> Set Accept Header To Application SDP Only
<input type="checkbox"/> Suppress End To End Session Refresh	<input type="checkbox"/> Set Oline Dash
<input type="checkbox"/> End To End PRACK	<input type="checkbox"/> Set Session Version Zero
<input type="checkbox"/> Enable Default PUI Procedures	<input type="checkbox"/> Set Sline Dash
<input type="checkbox"/> Enable Dial String Handling	<input type="checkbox"/> Store P-Charging Function Addr
<input type="checkbox"/> Include G729 with G729A when offer PSP has G729A	<input checked="" type="checkbox"/> Store P-Charging Vector
<input type="checkbox"/> Include IP Ports In FROM And TO Headers	<input type="checkbox"/> Store Path Header
<input type="checkbox"/> Include Reason Header (Q.850)	<input type="checkbox"/> Store Service-Route Header
<input type="checkbox"/> Include SS Attribute In Initial Invite	<input type="checkbox"/> Suppress Min-SE if not received
<input type="checkbox"/> Include Transport Type In Contact Header	<input type="checkbox"/> Terminal Portability Interworking
<input type="checkbox"/> Insert Peer Address As Top Route Header	<input type="checkbox"/> Send RTCP BandWidth Info
<input type="checkbox"/> Lockdown Preferred Codec	<input type="checkbox"/> Validate Access Nw Info Header
<input type="checkbox"/> Map Cause Location	<input type="checkbox"/> Use Psx Route for Registered Invite
<input type="checkbox"/> Map SGD In P-Sig-Info Header	<input type="checkbox"/> From Header Anonymisation
<input type="checkbox"/> Map Suspend/Resume Event In P-Svc-Info Header	<input type="checkbox"/> Create ISUP Message Body
<input type="checkbox"/> Map UUI In P-Sig-Info Header	<input type="checkbox"/> Disable Transparently Passing ISUP Message Body
<input type="checkbox"/> MIME Cause Precede Reason Header Cause	<input type="checkbox"/> aiToPcmInterworking

Relay Flags

<input type="checkbox"/> Conference Event Package	<input type="checkbox"/> PUBLISH
<input type="checkbox"/> Dialog Event Package	<input type="checkbox"/> REFER
<input type="checkbox"/> DTMF Body	<input type="checkbox"/> Reg Event Package
<input type="checkbox"/> Force 503 To 500 Relay	<input type="checkbox"/> Ribbon Media Body
<input type="checkbox"/> Info	<input type="checkbox"/> Status Code 3XX
<input type="checkbox"/> Message	<input type="checkbox"/> Status Code 4XX-6XX
<input type="checkbox"/> Notify	<input type="checkbox"/> Third Party Bodies
<input type="checkbox"/> Options	<input type="checkbox"/> Update without SDP

Refer To Header Relay

Reject the REFER request if no match is found
 relay the REFER request if no match is found
 relay the REFER request without matching

Transparency Flags

<input type="checkbox"/> Accept-Contact Header	<input type="checkbox"/> Reason Header
<input type="checkbox"/> Accept-Language Header	<input type="checkbox"/> Referred-By Header
<input type="checkbox"/> Accept Header	<input type="checkbox"/> Resource Priority Option Tag
<input type="checkbox"/> Alert Information Header	<input type="checkbox"/> Request-URI
<input type="checkbox"/> Allow Header	<input type="checkbox"/> Resource-Lists Body
<input type="checkbox"/> Authcode Headers	<input type="checkbox"/> RLMI Body
<input type="checkbox"/> Call-Info Header	<input type="checkbox"/> Route Header
<input type="checkbox"/> Contact Header*	<input type="checkbox"/> Server Header

Egress IP Attributes - Sending A Call In The Forward Direction To The Peer

IP Protocol Type: SIP Only SIP-I H.323 Wireless

IP Signaling MIME Content Type: ISUP

IP Signaling Treatment: Interwork

MIME Content Type Version: 1 - ansi88

Globalize Number Profile: <None>

Phone-Context Parameter Length: 0

Media Qos Kpi Profile: <None>

Signaling Qos Kpi Profile: <None>

Flags

<input type="checkbox"/> Accept 3XX With RN	<input type="checkbox"/> Qos Based Routing
<input type="checkbox"/> BGCF Target Scheme Transparency	<input type="checkbox"/> Prefix RN to Dialed Digits
<input type="checkbox"/> Convert Inactive To Sendrecv	<input type="checkbox"/> Reject 3XX With IP
<input type="checkbox"/> Delay Cut Through	<input type="checkbox"/> Reject 3XX With TN
<input checked="" type="checkbox"/> Disable 2806 Compliance	<input type="checkbox"/> Same CallId For Required Authorization
<input type="checkbox"/> Disable Optional Register Parameters	<input type="checkbox"/> Transit PAI From Unregistered Peer
<input checked="" type="checkbox"/> Disposition Handling Required	<input type="checkbox"/> Suppress UNREGISTER
<input type="checkbox"/> Don't Send Fast Start Proposal	<input type="checkbox"/> TTC-ISUP Mapping
<input type="checkbox"/> Enable 3261 Cancel Handling	<input type="checkbox"/> Use Called Party In Request URI
<input type="checkbox"/> Include ENUM Parameters	<input type="checkbox"/> Use Colon In SDP Media Type Parameter

Privacy

Transparency

AnonymizeHostIpAddress

Privacy Information: P-Preferred-ID P-Asserted-ID Remote-Party-ID

Flags

Include Privacy Privacy Required by Proxy

MS Lync Privacy Support Include Embedded PAI Header in Redirected INVITE

Do Not Include Tel URI In PAI Header

Redirect

Mode: ▾

Contact Handling: Merge Received Contacts with Existing Contacts Purge Existing Contacts

Flags

Skip Crankback Profile And Always Crankback Honor Embedded Headers in 3xx

Force Re-query for Redirection Enhanced Local Redirection

SIP Cause Mapping

Internal To SIP Cause Mapping: ▾

SIP To Internal Cause Mapping: ▾

Internal to SIP Cause Mapping Profile Name

SIP to Internal Cause Mapping Profile Name

Call Forwarding

Diversion-History Info Interworking (RFC 6044 compliance)

Redirection Information

Diversion Diversion With Transparency

PK Header

History Information

Include History-Info Cause Parameter In RFC 4458 Reason With Cause Value As Per RFC 4244

CPC Mapping Flags

Map CPC when Presentation Indicator is Restricted

Any CPC CPC=Priority

Send CPC Param In

Default PAI From Both (PAI and From)

P Charge Info

Transparency

P-Charge-Info Information: URI Parameter User Parameter Header Parameter

Flags

Include NPI Include NOA

Transport Type

Transport Type 1: <None>

Transport Type 2: <None>

Transport Type 3: <None>

Transport Type 4: <None>

Use configured transport for egress leg

Ingress IP Attributes - Signaling Back A Message To The Peer That We Receive A Call From

Flags

181 Supported

182 Supported

Convert Progress To Alert

Don't Send Facility Message

Don't Send 3XX With IP

Don't Send 3XX With TN

Map Called Party Category In P-Sig-Info Header

No SDP In 180 Supported

Refuse Fast Start Proposal

Registration Expires in Expires Header

Map Subsequent 180 to 183

Early Media Authorization

Registration Support 3xx

Send 183 On Initiating Disconnect Treatment

Send Fast Start Response In CP

Send SDP In 200 OK If 18x Reliable

Send Updated SDP In 200 OK

Send SDP In Subsequent 18x

Send TLS Connection Failure Response

Suppress 183 For 3xx Redirect Response

Suppress 183 Without SDP

Override 3xx Relay

Send BIT-H Of BCI In Outgoing Invite

Convert Alert To Progress

Save Cancel Delete

Packet Service Profile (PSP)

Create a Packet Service Profile (PSP) for the PSTN leg. The PSP is attached to the TrunkGroup that is created later in this section.

Figure 12: Packet Service Profile

Packet Service Profile: PSTN_PSP

Silence Factor: 40

Voice Initial Playout Buffer Delay (ms): 10

Type Of Service: 0

AAL1 Payload Size: 47

Preferred RTP Payload Type For DTMF Relay: <None>

Media Packet COS: 0

Monitoring Profile: <None>

Codec Entry

Codec Entry: <None>

Add Update

Codec Entry	Value
1	G711Ulaw_T38_2833

Delete

Media Control: IPv4 Only

Packet-To-Packet Control

Transcode: Only Conditional Determined By PSP For Other Leg Transcode

Conditions In Addition To "No Common Codec"

Apply Fax Tone Treatment Different Silence Suppression

Different DTMF Relay Honor Answer Preference

Different Packet Size Honor Offer Preference

Different 2833 Payload Type

Codecs Allowed For Transcoding

This Leg: G.711 A G.711 U G.722 G.722.2 G.723.1 G.726 G.729 OPUS EVS SILK T.38 iLBC AMR

Other Leg: G.711 A G.711 U G.722 G.722.2 G.723.1 G.726 G.729 OPUS EVS SILK T.38 iLBC AMR

RTCP

RTCP Packet Loss Threshold (Packets Lost/100,000 Packets): 0

RR Bandwidth: 250

RS Bandwidth: 250

Packet Loss Action: None Trap Trap And Disconnect

Enable RTCP Only For HELD Calls Termination For Pass-Through Calls

RTCP-MUX Generate RTCP for T140 if not received from other leg

RTCP-XR

Relay Relay Or Terminate

Peer Absence Action

None Trap Trap And Disconnect

Silence Insertion Descriptor

G.711 Silence Insertion Descriptor RTP Payload Type: 13

Silence Insertion Descriptor Heartbeat

Data Calls

Initial Playout Buffer Delay (ms): 50

Packet Size: 20

Preferred RTP Payload Type: 56

Video Calls

Maximum Video Bandwidth (kbps): 0

Video Bandwidth Reduction Factor (%): 0

Audio Only If Video Is Prevented

IPv4 TOS: 0

IPv6 Traffic Class: 0

IEEE 802.1Q VLAN COS: 0

Codec List Profile: <None>

Qos Values

MSRP DSCP: 0

DTLS SCTP DSCP: 0

T140 DSCP: 0

Application Dscp: 0

Secure RTP/RTCP

Crypto Suite Profile: <None>

Flags

Allow Fallback Enable SRTP

Reset ROC On Session Key Change Reset Enc/Dec/ROC on Decryption Key Change

Update Crypto On Modify Allow Pass Through

DTLS/SRTP

Crypto Suite Profile: <None>

Flags

Allow Fallback Enable DTLS

Relay DTLS SRTP Relay DTLS SCTP

Flags

DSCP Passthrough Interwork DTMF OOB-2833 Without Transcoding

Digit Detect Send Enabled Use Direct Media

Disallow Data Calls Validate Peer Support for DTMF Events

SSRC Randomize HD Codec Preferred

Reserve BW for Preferred Audio Common Codec Prefer NB PassThru Over HDTranscode

Police on Heaviest Audio Codec Match Offered Codec Group If Nb Only

t140 Call Force Route PSP Order

Allow Audio Transcode For MultiStream Call Allow Mid Call SSRC Modification

Generate and Signal SSRC and CName

< >

Save Cancel Delete

Packet Service Profile ID Group

Create the Packet Service Profile ID Group and attach the Packet Service Profile created earlier.

Figure 13: Packet Service Profile ID Group

Packet Service Profile ID Group: PSTN

Packet Service Profile: PSTN_PSP

HPC Packet Service Profile: <None>

IP Signaling Peer Group

Add the PSTN IP Address as shown below:

Figure 14: IP Signaling Peer Group

IP Signaling Peer Group: PSTN_IPP

Description:

Flags

Send All Peer IP Addresses/FQDNs

Peer Group Data

Sequence Number: 0

IPv4 Address: 172 . 16 . . Port Number: 5060

IPv6 Address: 0 : 0 : 0 : 0 : 0 : 0 : 0 : 0 Port Number: 0

Server FQDN: Port Number: 0

In Service

Add/Update

Sequence Number	IP Address	Port Number	Server FQDN	Port Number	Send	Service Status
0	172.16. .	5060		0	IP Address	In Service

Trunk Group

Create a SIP Trunk Group towards the PSTN and assign corresponding profiles like LRBT, PSP, IPSP created in earlier steps.

Figure 15: Trunk Group

Trunk Group:	PSTN_TG	<input type="checkbox"/> Unrestricted
Gateway:	ZOOM	
Description:		
Auto Recall Profile:	<None>	
Call Processing Localization Variant:	North America	
Calling Area:	<None>	
Carrier:	0000	
Carrier Selection Priority:	<None>	
Country:	1 - USA, Canada and Caribbean	
DDI Range Profile:	<None>	
Destination Switch Type:	Access	
Direction:	Two Way	
Element Routing Priority Profile:	ZOOM_ERP	
Feature Control Profile:	DEFAULT_FC_ACCESS	
IP Signaling Profile:	PSTN_IPSP	
LATA:	<None>	
Local Recursion Profile:	<None>	
Maximum Satellite Hops:	Three or More Satellite Hops	
Network Data Partition:	0	
Network Data Net:	0	
Next Hop Domain:	<None>	
Number Analysis Profile:	<None>	
Number Length Enforcement:	<None>	

Originating Carrier:	<None>	
PPR Profile:	<None>	
Pseudo Carrier:	<None>	
Remote Sip Peer Type:	None	
Region:	<None>	
Routing Criteria Profile:	DEFAULT_IP	
SCP Business Service Group:	0	
Signaling Profile:	DEFAULT_IP_PROFILE	
Signaling Flag:	SIP	
SIP Domain:	<None>	
SIP Response Code Profile:	<None>	
TDM Type:	Other	
Tone And Announcement Profile:	ZOOM_LRBT	
Trunk Group COS:		
Trunk Group COS Profile:	<None>	
Trunk Group Domain:	<None>	
Trunk Number:		
Zone Index Profile:	DEFAULT	
ZZ Profile:	<None>	
Charge Band Profile:	<None>	

Ingress

Charge Indicator:

Default CPC:

Default OLIP:

Dial Plan Profile:

Forced OLIP Value:

In DM/PM Rule:

Info Transfer Capability Profile:

IP Version Preference:

ONI:

JIP:

NPA:

Numbering Plan:

In Policy Profile Group:

Flags

<input type="checkbox"/> Allow Hex Digits In Cdpn	<input type="checkbox"/> Non-Zero Video Bandwidth Based Routing for H.323
<input type="checkbox"/> Discard NPDI	<input type="checkbox"/> Non-Zero Video Bandwidth Based Routing for SIP
<input type="checkbox"/> Discard RN	<input type="checkbox"/> Overlap Dialing
<input type="checkbox"/> HD Preferred Routing	<input type="checkbox"/> TNS Circuit Code Based Routing
<input type="checkbox"/> HD Supported Routing	<input checked="" type="checkbox"/> Use IPTG Routing (Hop By Hop Routing) For Ingress

Egress

Out DM/PM Rule:

Out Policy Profile Group:

Trunk Context:

R-URI Host: R-URI Host Port:

Flags

<input type="checkbox"/> Disable Crankback
<input type="checkbox"/> Enable JIP Interwork
<input type="checkbox"/> Use Preferred Identity

Billing

Billing Plan:

Billing Information:

Default Billing Number:

Nature Of Address:

Numbering Plan Indicator:

Calling Party Number

Calling Party:

Nature Of Address:

Numbering Plan Indicator:

Presentation:

Flags

Do Not Use For Fallback Bearer Capability Out Of Service

Escaped Satellite Trunk

Use Sac NonSac Call Types For ZZ Profile

IPTG

IP Signaling Peer Group: PSTN_IPP

IP Peer Supported

Packet Service Profile ID Group: PSTN

Egress IP Signaling Profile: PSTN_IPSP

Packet Service Profile

Preferred Packet Service Profile ID Group: <None>

Destination Override

Traffic Management Options

Trunk Group Reservation Level 1: 10

Trunk Group Reservation Level 2: 5

VPN Information

Business Group: <None>

Business Location: <None>

Business Group From CLI

Services

Not Screened Screened - Normal Screened - Fraud

Class Of Service: DEFAULT_IP

Service Exception Profile: <None>

Save Cancel Delete

Routing Label

Configure the Routing Label as follows:

Routing Label: PSTN_RL

Destination

Ignore Do not Use Use

Route Prioritization Type

Sequence Proportion Round Robin All Proportion Least Cost Routing

Route Prioritization Type For Equal Cost Routes: Sequence

Use TAR Routes

TAR Route Prioritization Type

Sequence Proportion Round Robin All Proportion Least Cost Routing

Route Prioritization Type For Equal Cost Routes: Sequence

Local Routes

Pass Only Local Routes Prioritize Local Routes Do Nothing

Flags

Continue Number Translation Continue CNAM Translation No Connect Signal To Be Sent

Routes

Type	Endpoint 1	Endpoint 2	IP Peer	Sequence	Proportion	Status	TAR Action	TAR Loc...	DM/PM R...	Apply Later	Testing	Cost	Skip LR	STI Type
GSX Gate...	PSTN_TG	ZOOM		1	0	In Service	Normal	0		Do Not A...	Normal	1000000	Disabled	0

New Open Delete

Save Cancel Delete

Create a new Route and attach the Gateway and Trunk Group as created earlier.

Route

Type: GSX Gateway

Gateway: ZOOM

Trunk Group: PSTN_TG

IP Peer: <None>

Sequence: 1

Proportion: 0

Cost: 1000000

TAR Action: Normal

TAR Location: 0

DM/PM Rule: <None> Apply Later

Testing: Normal Test Non-Test

In Service Skip Local Recursion

Signing Local Tagging Verification

OK Cancel

Zoom Leg Configuration

IP Signaling Profile (IPSP)

Create an IP Signaling Profile with appropriate signaling flags towards Zoom.

Figure 16: IP Signaling Profile

Host: 172.16.100.216 @ 4330
 Master (SWE) - V12.02.02R000

View: IP Signaling Profile Close All Perspective: Full View

IP SIGNALING PROFILE: ZOOM_IPSP

Common IP Attributes - Communicating With The Peer Regardless Of Call Direction

<input type="checkbox"/> Accept Alert Info	<input type="checkbox"/> No Content Disposition
<input type="checkbox"/> Add P-Charging Function Addr	<input type="checkbox"/> No Port Number 5060
<input type="checkbox"/> Add Path/Service Route Per TG	<input type="checkbox"/> No Userinfo In Contact Header
<input type="checkbox"/> Audio Codec Change through Empty TCS	<input type="checkbox"/> Only Selected Codec In Session Refresh
<input type="checkbox"/> Call Hold Interworking	<input type="checkbox"/> Override Relay For Non SIP Egress Leg
<input type="checkbox"/> Calling Party Type Number If Present	<input checked="" type="checkbox"/> P-Called-Party-Id-Support
<input type="checkbox"/> Clearmode For Data Calls	<input type="checkbox"/> P-ChgMsg-Info
<input type="checkbox"/> Create P-Charging-Vector	<input type="checkbox"/> Relay Data Path Mode Changes To The Other Leg
<input type="checkbox"/> Create P-Visited-Network Id	<input type="checkbox"/> Reject REFER
<input type="checkbox"/> Create Path Header	<input type="checkbox"/> Replace Host On Via Header
<input type="checkbox"/> Create Service-Route Header	<input type="checkbox"/> Reject REFER With IP
<input type="checkbox"/> Customized Session Timer Behavior	<input type="checkbox"/> Reject REFER With TN
<input type="checkbox"/> Disable Also Header	<input type="checkbox"/> ReQuery PSX on REGISTER Refresh
<input type="checkbox"/> Disable Constrained Capacities	<input type="checkbox"/> Restrict History Info Header
<input type="checkbox"/> Disable Host Translation	<input type="checkbox"/> Route Using Received FQDN
<input type="checkbox"/> Disable Media Lock Down	<input type="checkbox"/> SDP O-line Only Compares
<input type="checkbox"/> Disable Refer-To URI Parameters	<input type="checkbox"/> Send All Allowed Codecs For Late Media Invite Or Re-Invite
<input type="checkbox"/> Discard Received Reason Header	<input type="checkbox"/> Send Direct Media Info In SDP Attribute
<input type="checkbox"/> Do Not Include SS Attribute In Re-INVITE	<input type="checkbox"/> Send Empty TCS

<input type="checkbox"/> Don't Send REFER With IP	<input type="checkbox"/> Send Only Preferred Codec
<input type="checkbox"/> Don't Send REFER With TN	<input type="checkbox"/> Send PTIME In SDP
<input type="checkbox"/> End To End BYE	<input type="checkbox"/> Send RTCP Port In SDP
<input type="checkbox"/> End To End RE-INVITE	<input type="checkbox"/> Session Timer Refresh Update
<input type="checkbox"/> End To End UPDATE	<input type="checkbox"/> Set Accept Header To Application SDP Only
<input type="checkbox"/> Suppress End To End Session Refresh	<input type="checkbox"/> Set Oline Dash
<input type="checkbox"/> End To End PRACK	<input type="checkbox"/> Set Session Version Zero
<input type="checkbox"/> Enable Default PUI Procedures	<input type="checkbox"/> Set Sline Dash
<input type="checkbox"/> Enable Dial String Handling	<input type="checkbox"/> Store P-Charging Function Addr
<input type="checkbox"/> Include G729 with G729A when offer PSP has G729A	<input checked="" type="checkbox"/> Store P-Charging Vector
<input type="checkbox"/> Include IP Ports In FROM And TO Headers	<input type="checkbox"/> Store Path Header
<input type="checkbox"/> Include Reason Header (Q.850)	<input type="checkbox"/> Store Service-Route Header
<input type="checkbox"/> Include SS Attribute In Initial Invite	<input type="checkbox"/> Suppress Min-SE if not received
<input type="checkbox"/> Include Transport Type In Contact Header	<input type="checkbox"/> Terminal Portability Interworking
<input type="checkbox"/> Insert Peer Address As Top Route Header	<input type="checkbox"/> Send RTCP BandWidth Info
<input type="checkbox"/> Lockdown Preferred Codec	<input type="checkbox"/> Validate Access Nw Info Header
<input type="checkbox"/> Map Cause Location	<input type="checkbox"/> Use Psx Route for Registered Invite
<input type="checkbox"/> Map SGD In P-Sig-Info Header	<input type="checkbox"/> From Header Anonymisation
<input type="checkbox"/> Map Suspend/Resume Event In P-Svc-Info Header	<input type="checkbox"/> Create ISUP Message Body

<input type="checkbox"/> Map UII In P-Sig-Info Header	<input type="checkbox"/> Disable Transparently Passing ISUP Message Body
<input type="checkbox"/> MIME Cause Precede Reason Header Cause	<input type="checkbox"/> aiToPemInterworking
<input type="checkbox"/> Minimize Relaying Of Media Changes From Other Call Leg	<input type="checkbox"/> Send SBC Supported Codecs For Late Media Re-Invite
<input type="checkbox"/> No Service Route Hdr For Emergency Registration	
<input type="checkbox"/> Publish IP In Hold SDP	
<input type="checkbox"/> Insert PAccess Network Info	
<input type="checkbox"/> Contact Transparency For Isfocus Media Tag	
<input type="checkbox"/> Support S-CSCF Restoration Procedures	
<input type="checkbox"/> Insert UE Flow Info	
<input type="checkbox"/> Include SIP Reason Header	
Call Preservation Flags	
<input type="checkbox"/> Call Preservation	
Call Preservation Time Out: 5	
Call Transfer Flags	
Handle IP Addresses Not Present In Network Selector Table (NST): Route Via Transferring IPTG	
<input type="checkbox"/> Force Re-Route Via PSX Query	
<input type="checkbox"/> Skip Re-Route Via PSX Query	
Local Media Control Flags	
<input type="checkbox"/> Enable HOLD on REFER	
Option Tag In Require Header	
<input type="checkbox"/> Suppress Replace Tag	

PreConditions Profile	
<input type="checkbox"/> State	<input type="checkbox"/> Strength Optional Policy
<input type="checkbox"/> Support If Egress IPTG	<input type="checkbox"/> UPDATE Preconditions Policy
<input type="checkbox"/> Strength Mandatory Policy	
Strength Mandatory Priority:	1
Strength Optional Priority:	1
UPDATE Preconditions Priority:	1
Relay Flags	
<input type="checkbox"/> Conference Event Package	<input type="checkbox"/> PUBLISH
<input type="checkbox"/> Dialog Event Package	<input type="checkbox"/> REFER
<input type="checkbox"/> DTMF Body	<input type="checkbox"/> Reg Event Package
<input type="checkbox"/> Force 503 To 500 Relay	<input type="checkbox"/> Ribbon Media Body
<input type="checkbox"/> Info	<input type="checkbox"/> Status Code 3XX
<input type="checkbox"/> Message	<input type="checkbox"/> Status Code 4XX-6XX
<input type="checkbox"/> Notify	<input type="checkbox"/> Third Party Bodies
<input type="checkbox"/> Options	<input type="checkbox"/> Update without SDP
Refer To Header Relay	
<input checked="" type="radio"/> Reject the REFER request if no match is found <input type="radio"/> relay the REFER request if no match is found <input type="radio"/> relay the REFER request without matching	
Transparency Flags	
<input type="checkbox"/> Accept-Contact Header	<input type="checkbox"/> Reason Header
<input type="checkbox"/> Accept-Language Header	<input type="checkbox"/> Referred-By Header

<input type="checkbox"/> Accept Header	<input type="checkbox"/> Resource Priority Option Tag
<input type="checkbox"/> Alert Information Header	<input type="checkbox"/> Request-URI
<input type="checkbox"/> Allow Header	<input type="checkbox"/> Resource-Lists Body
<input type="checkbox"/> Authcode Headers	<input type="checkbox"/> RLMl Body
<input type="checkbox"/> Call-Info Header	<input type="checkbox"/> Route Header
<input type="checkbox"/> Contact Header*	<input type="checkbox"/> Server Header
<input type="checkbox"/> Error Info	<input type="checkbox"/> Service-Route Header
<input type="checkbox"/> Event Header	<input type="checkbox"/> Simple-Filter Body
<input type="checkbox"/> External Body	<input type="checkbox"/> SIP Body
<input type="checkbox"/> From Header	<input type="checkbox"/> SIPFRAG Body
<input type="checkbox"/> Geo Location Error	<input type="checkbox"/> Target-Dialog Header
<input type="checkbox"/> Geo Location Header	<input type="checkbox"/> To Header
<input type="checkbox"/> Geo Location Route	<input type="checkbox"/> Tone Body
<input type="checkbox"/> History Info	<input type="checkbox"/> Unknown Body
<input type="checkbox"/> Image Body	<input type="checkbox"/> Unknown Header
<input type="checkbox"/> Max_forwards Header	<input type="checkbox"/> User-Agent Header
<input type="checkbox"/> MWI Body	<input type="checkbox"/> User-To-User Header
<input type="checkbox"/> Pass Complete Contact Header	<input type="checkbox"/> Via Header
<input type="checkbox"/> P-Access-Network-Info Header	<input type="checkbox"/> Warning Header
<input type="checkbox"/> P-Called-Party-Id	<input type="checkbox"/> Watcherinfo Body

<input type="checkbox"/> P-Charging-Vector Header	<input type="checkbox"/> X-ATP
<input type="checkbox"/> P-Early-Media	
<input type="checkbox"/> P-Visited-Network ID Header	
<input type="checkbox"/> Path Header	
<input type="checkbox"/> Pdf Body	
<input type="checkbox"/> Pdf-Diff Body	
<input type="checkbox"/> QSIG Body	
PDCCS-Billing Info Header	
<input type="checkbox"/> Transparency	
<input type="checkbox"/> Include Privacy	
Sip In Core	
	<input type="checkbox"/> Use SIP In Core
Header Encryption Flags	
<input type="checkbox"/> Path Header	<input type="checkbox"/> Service Route Header
Subscription Package Support	
<input type="checkbox"/> Support Reg Event	<input type="checkbox"/> Use PSX Route For SBC Initiated Subscribe
Registrar Recovery	
<input type="checkbox"/> Register to Alternate on Primary Down	<input type="checkbox"/> Override Internal Expires Timer
<input type="checkbox"/> Revert to Primary On Recovery	<input type="checkbox"/> Deregister Alternate on Primary Recovery
Egress IP Attributes - Sending A Call In The Forward Direction To The Peer	

Egress IP Attributes - Sending A Call In The Forward Direction To The Peer

IP Protocol Type: SIP Only SIP-I H.323 Wireless

IP Signaling MIME Content Type: ISUP

IP Signaling Treatment: Interwork

MIME Content Type Version: 1 - ansi88

Globalize Number Profile: DEFAULT_IP

Phone-Context Parameter Length: 0

Media Qos Kpi Profile: <None>

Signaling Qos Kpi Profile: <None>

Flags

<input type="checkbox"/> Accept 3XX With RN	<input type="checkbox"/> Qos Based Routing
<input type="checkbox"/> BGCF Target Scheme Transparency	<input type="checkbox"/> Prefix RN to Dialed Digits
<input type="checkbox"/> Convert Inactive To Sendrecv	<input type="checkbox"/> Reject 3XX With IP
<input type="checkbox"/> Delay Cut Through	<input type="checkbox"/> Reject 3XX With TN
<input checked="" type="checkbox"/> Disable 2806 Compliance	<input type="checkbox"/> Same CallId For Required Authorization
<input type="checkbox"/> Disable Optional Register Parameters	<input type="checkbox"/> Transit PAI From Unregistered Peer
<input checked="" type="checkbox"/> Disposition Handling Required	<input type="checkbox"/> Suppress UNREGISTER
<input type="checkbox"/> Don't Send Fast Start Proposal	<input type="checkbox"/> TTC-ISUP Mapping
<input type="checkbox"/> Enable 3261 Cancel Handling	<input type="checkbox"/> Use Called Party In Request URI
<input type="checkbox"/> Include ENUM Parameters	<input type="checkbox"/> Use Colon In SDP Media Type Parameter
<input type="checkbox"/> Insert In Band Indication	<input type="checkbox"/> Use JIP from 3XX Response in PDCS-Billing-Info-Header

<input type="checkbox"/> Add Loop Back Route Header	<input type="checkbox"/> Validate ISUB Address
<input type="checkbox"/> Map 181 Or 182 Message To 183	<input type="checkbox"/> Wait Till Connect Before Abandon FastStart
<input type="checkbox"/> Map 3xx Contact URL To Route Header	<input type="checkbox"/> Restrict User Equal To Phone
<input type="checkbox"/> Map Contractor Number In P-Sig-Info Header	<input type="checkbox"/> Ignore SDP After Offer Answer Completed
<input type="checkbox"/> Use Network Provided Screening Indicator For Calling Number	<input type="checkbox"/> Map Diversion Header To Charge Number
<input type="checkbox"/> MonitorRtpOnEgressUpdate	<input type="checkbox"/> Map RN, OCN, RDI To Diversion Header
<input type="checkbox"/> Honor Subsequent SDP Answer	

BCI

<input type="checkbox"/> BCI Interwork Encountered	<input type="checkbox"/> BCI ISDN Access
--	--

Carrier Information

<input type="checkbox"/> Disconnect If Neither Terminating CA Nor CIC Received	<input type="checkbox"/> Use Terminating CIC From SIP
<input type="checkbox"/> Use Terminating CA From SIP	

Domain Name

<input type="checkbox"/> Preserve Ingress FROM Domain Name	<input type="checkbox"/> Use Lower Case Domain Names
<input type="checkbox"/> Preserve Ingress R-URI Domain Name	<input type="checkbox"/> Use SIP Domain Name In FROM Field
<input type="checkbox"/> Use IP Signaling Peer Domain In R-URI	<input type="checkbox"/> Use Zone Level Domain Name In Contact
<input type="checkbox"/> Use DM/PM Manipulated Host Name In R-URI	<input type="checkbox"/> Use SIP Domain Name In Request URI
<input type="checkbox"/> Use Zone Level Domain Name In Path Header	<input type="checkbox"/> Use Called URI As R-URI
<input type="checkbox"/> Use SIP Domain Name In PAI Header	

ISUB

IP SIGNALING PROFILE: ZOOM_IPSP

- Allow NSAP ISUB
- Allow User Specified ISUB
- Include Called Party ISUB
- Include Calling Party ISUB

Number Portability Attributes

- NPDI Options: Include npdi Include npdi=yes Do Not Include npdi

Flags

- Disable rn

Privacy

- Transparency
- AnonymizeHostIpAddress

- Privacy Information: P-Preferred-ID P-Asserted-ID Remote-Party-ID

Flags

- Include Privacy
- MS Lync Privacy Support
- Do Not Include Tel URI In PAI Header
- Privacy Required by Proxy
- Include Embedded PAI Header in Redirected INVITE

Redirect

Mode: Accept Redirection

- Contact Handling: Merge Received Contacts with Existing Contacts Purge Existing Contacts

Flags

- Skip Crankback Profile And Always Crankback
- Force Re-query for Redirection
- Honor Embedded Headers in 3xx
- Enhanced Local Redirection

SIP Cause Mapping

Internal To SIP Cause Mapping: 1 - DEFAULT

SIP To Internal Cause Mapping: 1 - DEFAULT

Internal to SIP Cause Mapping Profile Name

SIP to Internal Cause Mapping Profile Name

SIP Headers And Parameters

- Include Charge Information: Include None Include P-Charge-Info

- Session-Expires Refresher: Not Send UAC UAS

- SIP TO Header Mapping: None Original Called Number (OCN) Called Number GAP Dialed Number

- PI Allowed Send CPC In: DEFAULT FROM PAI BOTH

Destination Trunk Group Options: Include None

Originating Trunk Group Options: Include None

Generate Call-ID Using: Do not Use Ingress Call-Id

Flags

- Include CIC
- Include CPC Information
- Include NPI
- Include OLIP
- Include P-K-Adn
- Include PSTN Parameters
- Include Qvalue
- Skip CSeq Check In Early Dialog
- Transparency For Destination Trunk Group Parameter
- End To End Ack
- No CDR Change In End To End Ack

Call Forwarding

Diversion-History Info Interworking (RFC 6044 compliance)

Redirection Information

Diversion Diversion With Transparency

PK Header

History Information

Include History-Info Cause Parameter In RFC 4458 Reason With Cause Value As Per RFC 4244

CPC Mapping Flags

Map CPC when Presentation Indicator is Restricted

Any CPC CPC=Priority

Send CPC Param In

Default PAI From Both (PAI and From)

P Charge Info

Transparency

P-Charge-Info Information: URI Parameter User Parameter Header Parameter

Flags

Include NPI Include NOA

SIP RPH ETS

Action For ETS 400 Response With 417 Reason Code:

ETS Default Priority Value:

Flags

Add/Modify ETS Resource Priority Header Use Incoming ETS Resource Value

Do Not Include Require RPH

Transport Type

Transport Type 1:

Transport Type 2:

Transport Type 3:

Transport Type 4:

Use configured transport for egress leg

Ingress IP Attributes - Signaling Back A Message To The Peer That We Receive A Call From

Flags

<input type="checkbox"/> 181 Supported	<input type="checkbox"/> Registration Support 3xx
<input type="checkbox"/> 182 Supported	<input type="checkbox"/> Send 183 On Initiating Disconnect Treatment
<input type="checkbox"/> Convert Progress To Alert	<input type="checkbox"/> Send Fast Start Response In CP
<input type="checkbox"/> Don't Send Facility Message	<input type="checkbox"/> Send SDP In 200 OK If 18x Reliable
<input type="checkbox"/> Don't Send 3XX With IP	<input type="checkbox"/> Send Updated SDP In 200 OK
<input type="checkbox"/> Don't Send 3XX With TN	<input type="checkbox"/> Send SDP In Subsequent 18x
<input type="checkbox"/> Map Called Party Category In P-Sig-Info Header	<input type="checkbox"/> Send TLS Connection Failure Response
<input type="checkbox"/> No SDP In 180 Supported	<input type="checkbox"/> Suppress 183 For 3xx Redirect Response
<input type="checkbox"/> Refuse Fast Start Proposal	<input type="checkbox"/> Suppress 183 Without SDP

<input type="checkbox"/> Registration Expires in Expires Header	<input type="checkbox"/> Override 3xx Relay
<input type="checkbox"/> Map Subsequent 180 to 183	<input type="checkbox"/> Send BIT-H Of BCI In Outgoing Invite
<input type="checkbox"/> Early Media Authorization	<input type="checkbox"/> Convert Alert To Progress
<input type="checkbox"/> Report Early Media Auth	
Carrier Information	
<input type="checkbox"/> Generate Terminating CA	<input type="checkbox"/> Generate Terminating CIC
History Information	
<input type="checkbox"/> Include History-Info	<input type="checkbox"/> Cause Parameter In RFC 4458
	<input type="checkbox"/> Reason With Cause Value As Per RFC 4244
Access Transfer Profile: <None>	
Trf Parameters	
Preferred Trf Uri	
Preferred Mrb Uri	
Enum Parameters	
TTL	0
<input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Delete"/>	

Packet Service Profile (PSP)

Create a Packet Service Profile (PSP) for the Zoom leg. The PSP is attached to the TrunkGroup that is created later in this section. Since there is an SRTP between the SBC Core and Zoom, you must create a crypto suite profile as shown below:

Figure 17: Packet Service Profile

Packet Service Profile: ZOOM_PSP	
Silence Factor:	40
Voice Initial Playout Buffer Delay (ms):	10
Type Of Service:	0
AAL1 Payload Size:	47
Preferred RTP Payload Type For DTMF Relay:	<None>
Media Packet COS:	0
Monitoring Profile:	<None>
Codec Entry	
Codec Entry:	<None>
<input type="button" value="Add"/> <input type="button" value="Update"/>	
Codec Entry	Value
1	G711Ulaw_T38_2833

Media Control: IPv4 Only

T.38

Number of Redundant Packets 0 1

Low Speed Number of Redundant Packets 0 1

T.38v0 Maximum Bit Rate 2.4 kbits/s 4.8 kbits/s 9.6 kbits/s

Data Rate Management Type Type 1 - Local Generation of TCF Type 2 - Transfer of TCF

Use Max Bit Rate Only Disabled Enabled

ECM ECM Preferred

T.38FaxMaxDatagram Size without Redundancy Disabled Enabled

T.38FaxProtocolVersion: T.38(v0)

Honor Remote Precedence Disabled Enabled

Send Route PSP Precedence Disabled Enabled

Packet-To-Packet Control

Transcode Only Conditional Determined By PSP For Other Leg Transcode

Conditions In Addition To "No Common Codec"

Apply Fax Tone Treatment Different Silence Suppression

Different DTMF Relay Honor Answer Preference

Different Packet Size Honor Offer Preference

Different 2833 Payload Type

Codecs Allowed For Transcoding

This Leg: G.711 A G.711 U G.722 G.722.2 G.723.1 G.726 G.729 OPUS EVS SILK T.38 iLBC AMR

Other Leg: G.711 A G.711 U G.722 G.722.2 G.723.1 G.726 G.729 OPUS EVS SILK T.38 iLBC AMR

RTCP

RTCP Packet Loss Threshold (Packets Lost/100,000 Packets): 0

RR Bandwidth: 250

RS Bandwidth: 250

Packet Loss Action None Trap Trap And Disconnect

Enable RTCP Only For HELD Calls Termination For Pass-Through Calls

RTCP-MUX Generate RTCP for T140 if not received from other leg

RTCP-XR

Relay Relay Or Terminate

Secure RTP/RTCP
 Crypto Suite Profile: ZOOM_CRYPT

Flags

Allow Fallback Enable SRTP
 Reset ROC On Session Key Change Reset Enc/Dec/ROC on Decryption Key Change
 Update Crypto On Modify Allow Pass Through

DTLS/SRTP
 Crypto Suite Profile: <None>

Flags

Allow Fallback Enable DTLS
 Relay DTLS SRTP Relay DTLS SCTP

Flags

DSCP Passthrough Interwork DTMF OOB-2833 Without Transcoding
 Digit Detect Send Enabled Use Direct Media
 Disallow Data Calls Validate Peer Support for DTMF Events
 SSRC Randomize HD Codec Preferred
 Reserve BW for Preferred Audio Common Codec Prefer NB PassThru Over HDTranscode
 Police on Heaviest Audio Codec Match Offered Codec Group If Nb Only
 t140 Call Force Route PSP Order
 Allow Audio Transcode For MultiStream Call Allow Mid Call SSRC Modification
 Generate and Signal SSRC and CName

< Save Cancel Delete >

Packet Service Profile ID Group

Create a Packet Service Profile ID Group and attach the Packet Service Profile created earlier.

Figure 18: Packet Service Profile ID Group

Packet Service Profile ID Group: ZOOM

Packet Service Profile: ZOOM_PSP

HPC.Packet.Service.Profile: <None>

IP Signaling Peer Group

Add the Zoom IP Address as shown below:

Figure 19: IP Signaling Peer Group

IP Signaling Peer Group: ZOOM_IPP

Description:

Flags

Send All Peer IP Addresses/FQDNs

Peer Group Data

Sequence Number: 0

IPv4 Address: 162 . 12 . . Port Number: 5060
 IPv6 Address: 0 : 0 : 0 : 0 : 0 : 0 : 0 : 0 Port Number: 0
 Server FQDN: Port Number: 0

In Service

Add/Update

Sequence Number	IP Address	Port Number	Server FQDN	Port Number	Send	Service Status
0	162.12 . .	5060		0	IP Address	In Service

Trunk Group

Create a SIP Trunk Group towards Zoom and assign the corresponding profiles like LRBT, PSP, IPSP created in earlier steps.

Figure 20: Trunk Group

Trunk Group:	ZOOM_TG	<input type="checkbox"/> Unrestricted
Gateway:	ZOOM	
Description:		
Auto Recall Profile:	<None>	
Call Processing Localization Variant:	North America	
Calling Area:	<None>	
Carrier:	0000	
Carrier Selection Priority:	<None>	
Country:	1 - USA, Canada and Caribbean	
DDI Range Profile:	<None>	
Destination Switch Type:	Access	
Direction:	Two Way	
Element Routing Priority Profile:	ZOOM_ERP	
Feature Control Profile:	DEFAULT_SIP_FC_ACCESS	
IP Signaling Profile:	ZOOM_IPSP	
LATA:	<None>	
Local Recursion Profile:	<None>	
Maximum Satellite Hops:	Three or More Satellite Hops	
Network Data Partition:	0	
Network Data Net:	0	
Next Hop Domain:	<None>	
Number Analysis Profile:	<None>	
Number Length Enforcement:	<None>	

Originating Carrier:	<None>	
PPR Profile:	<None>	
Pseudo Carrier:	<None>	
Remote Sip Peer Type:	None	
Region:	<None>	
Routing Criteria Profile:	DEFAULT_IP	
SCP Business Service Group:	0	
Signaling Profile:	DEFAULT_IP_PROFILE	
Signaling Flag:	SIP	
SIP Domain:	<None>	
SIP Response Code Profile:	<None>	
TDM Type:	Other	
Tone And Announcement Profile:	ZOOM_LRBT	
Trunk Group COS:		
Trunk Group COS Profile:	<None>	
Trunk Group Domain:	<None>	
Trunk Number:		
Zone Index Profile:	DEFAULT	
ZZ Profile:	<None>	
Charge Band Profile:	<None>	

Ingress

Charge Indicator:

Default CPC:

Default OLIP:

Dial Plan Profile:

Forced OLIP Value:

In DM/PM Rule:

Info Transfer Capability Profile:

IP Version Preference:

ONI:

JIP:

NPA:

Numbering Plan:

In Policy Profile Group:

Flags

Allow Hex Digits In Cdpn

Discard NPDI

Discard RN

HD Preferred Routing

HD Supported Routing

Non-Zero Video Bandwidth Based Routing for H.323

Non-Zero Video Bandwidth Based Routing for SIP

Overlap Dialing

TNS Circuit Code Based Routing

Use IPTG Routing (Hop By Hop Routing) For Ingress

Egress

Charge Indicator:

Out DM/PM Rule:

Out Policy Profile Group:

Trunk Context:

R-URI Host: R-URI Host Port:

Flags

Disable Crankback

Enable JIP Interwork

Use Preferred Identity

Billing

Billing Plan:

Billing Information:

Default Billing Number:

Nature Of Address:

Numbering Plan Indicator:

Calling Party Number

Calling Party:

Nature Of Address:

Numbering Plan Indicator:

IP Signaling Peer Group: ZOOM_IPP IP Peer Supported

Packet Service Profile ID Group: ZOOM

Egress IP Signaling Profile: ZOOM_IPSP

Packet Service Profile

Preferred Packet Service Profile ID Group: <None> Destination Override

Traffic Management Options

Trunk Group Reservation Level 1: 10

Trunk Group Reservation Level 2: 5

VPN Information

Business Group: <None>

Business Location: <None> Business Group From CLI

Services

Not Screened Screened - Normal Screened - Fraud

Class Of Service: DEFAULT_IP

Service Exception Profile: <None>

Save Cancel Delete

Routing Label

Configure the Routing Label as follows:

Figure 21: Routing Label

Routing Label: ZOOM_RL

Action

Routes Script Route Hopping LCR

Number Of Routes Requested: 10 All

Number Of Routes Per Call: 10

Script: <None> [Runtime Variables](#)

Partition: <None>

DM/PM Rule: <None> Apply Later

CPC Screening: <None>

Overflow Number:

Overflow Nature Of Address: <None>

Overflow Numbering Plan Indicator: <None>

Call Parameter Filter Group: <None>

Call Parameter Filter Profile Script: <None>

Routing Criteria

Use Entity Type <None>

Partition

Ignore Do not Use Use

Destination

Ignore Do not Use Use

Route Prioritization Type

Sequence Proportion Round Robin All Proportion Least Cost Routing

Route Prioritization Type For Equal Cost Routes: Sequence

Use TAR Routes

TAR Route Prioritization Type

Sequence Proportion Round Robin All Proportion Least Cost Routing

Route Prioritization Type For Equal Cost Routes: Sequence

Local Routes

Pass Only Local Routes Prioritize Local Routes Do Nothing

Flags

Continue Number Translation Continue CNAM Translation No Connect Signal To Be Sent

Routes

Type	Endpoint 1	Endpoint 2	IP Peer	Sequence	Proportion	Status	TAR Action	TAR Loc...	DM/PM R...	Apply Later	Testing	Cost	Skip LR	STI Type
GSX Gate...	ZOOM_TG	ZOOM		1	0	In Service	Normal	0		Do Not A...	Normal	1000000	Disabled	0

New Open Delete

Create a new Route and attach the Gateway and Trunk Group as created earlier.

Route ✕

Type: GSX Gateway

Gateway: ZOOM

Trunk Group: ZOOM_TG

IP Peer: <None>

Sequence: 1

Proportion: 0

Cost: 1000000

TAR Action: Normal

TAR Location: 0

DM/PM Rule: <None> Apply Later

Testing: Normal Test Non-Test

In Service Skip Local Recursion

Signing Local Tagging Verification

OK Cancel

Standard Route

PSX uses this entry to route all the calls coming from the PSTN towards ZOOM End Points.

Figure 22: Standard Route 1

Entity Type: Trunk Group

Trunk Group: PSTN_TG All

GATEWAY: ZOOM

Not Applicable

Call Parameter Filter Profile: <None>

Call Parameter Filter Profile Group: <None>

Destination National:

Destination Country: 1 - USA, Canada and Caribbean

Domain Name: <None>

IP Address: 0 . 0 . 0 . 0

Partition: DEFAULT

Routing Label: ZOOM_RL

Call Type

Transmission Medium

- Speech
- 3.1 KHz Audio
- 7.0 KHz Audio
- 56 kbps
- 64 kbps
- Packet
- Multirate
- 384 kbps
- 1536 kbps

All Call Type Bits

Time Range: ALL

Always Confirm Changes

PSX uses this entry to route all the calls coming from ZOOM towards PSTN End Points.

Figure 23: Standard Route 2

Entity Type: Trunk Group

Trunk Group: ZOOM_TG All

GATEWAY: ZOOM

Not Applicable

Call Parameter Filter Profile: <None>

Call Parameter Filter Profile Group: <None>

Destination National:

Destination Country: 1 - USA, Canada and Caribbean

Domain Name: <None>

IP Address: 0 . 0 . 0 . 0

Partition: DEFAULT

Routing Label: PSTN_RL

Call Type

Transmission Medium

- Speech
- 3.1 KHz Audio
- 7.0 KHz Audio
- 56 kbps
- 64 kbps
- Packet
- Multirate
- 384 kbps
- 1536 kbps

All Call Type Bits

Time Range: ALL

Always Confirm Changes

Section D: Zoom Web BYOC Configuration

Prerequisites :

- **Zoom Go BYOC account:** This is a special type of Zoom account that has an 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 and the carrier equipment can be router/gateway or another SBC that supports SIP trunk connectivity. The carrier provides several DID's to use as external BYOC numbers.
- **Trunk Registration:** BYOC is a "static" trunk between two static IP endpoints, therefore no trunk registration is done here.



Note

Ensure a Zoom BYOC SIP trunk is built between the Zoom SBC and the Ribbon SBC Core deployed on a customer site.

Once the Zoom Go account is available, login to the 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

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

Figure 24: Add External Number

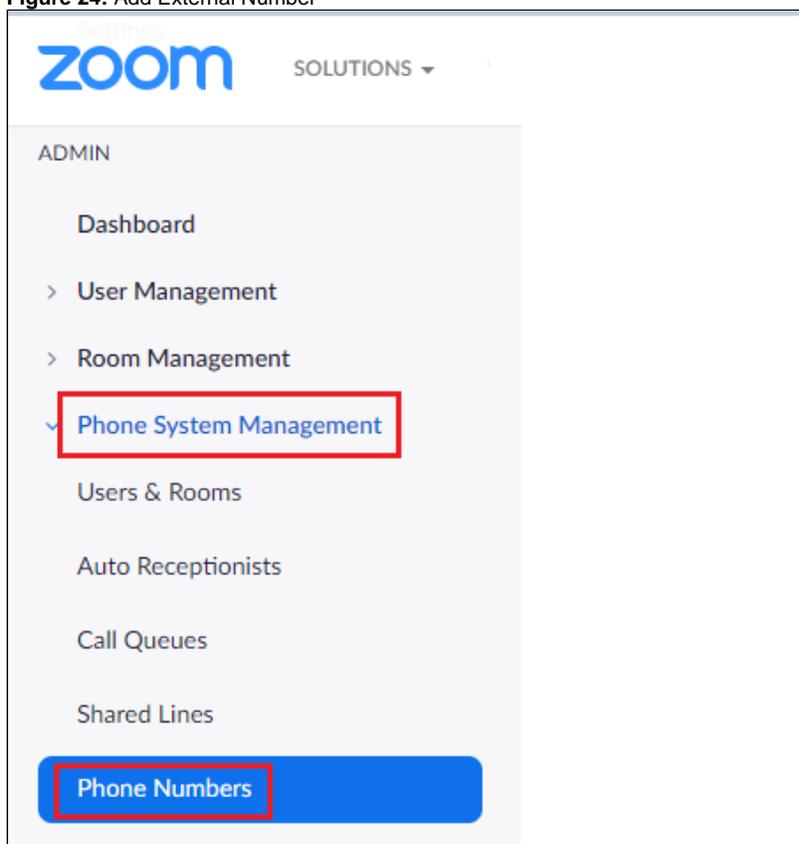
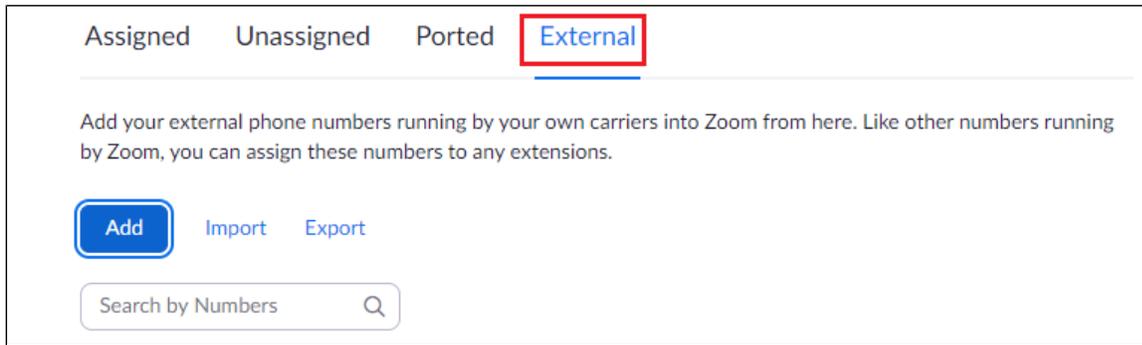


Figure 25: External



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

Figure 26: Add External Number

Enter the existing customer phone numbers (from carrier) separated by commas.

4. Click **Submit**.
5. Verify the external numbers have been created successfully as shown below.

Figure 27: External Number created successfully

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 desktop or mobile. The steps for creating a user are as follows:

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

Figure 28: Create Zoom User

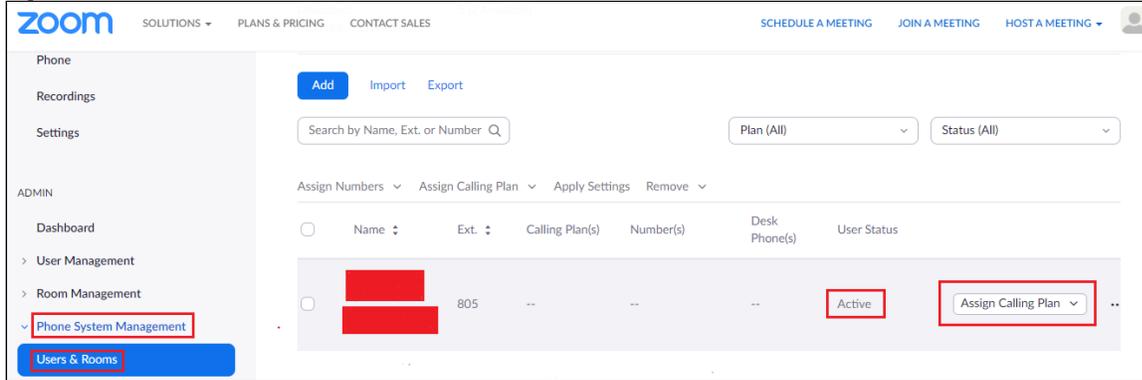
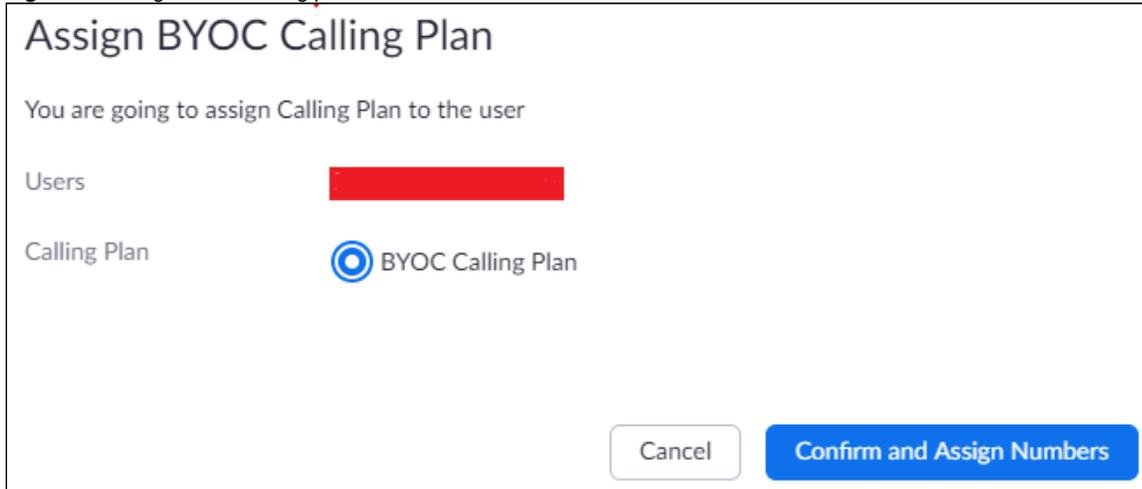


Figure 29: Assign BYOC calling plan



7. Assign the External Numbers created previously in [Add External Number](#).

Figure 30: Choose from Unassigned Numbers

Choose from Unassigned External Numbers

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

Page Size:
Total 1

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

Figure 31: Configured User

Import Export

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	BYOC	(512) 567-1233 E	--	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
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/>

Supplementary Services & Features Coverage

The following checklist depicts the set of services/features covered through the configuration defined in this Interop Guide.

Sr.No.	Supplementary Features/Services	Coverage
1	Basic Registration over UDP, TCP & TLS	N/A

2	Basic Call Setup	✓
3	Basic Call Termination	✓
4	Auto Receptionist (Auto Attendant)	✓
5	Call Waiting	✓
6	Call Hold/Resume	✓
7	Call Transfer - Blind (Cold Transfer)	✓
8	Call Transfer - Consult (Warm Transfer)	✓
9	Call Queue	✓
10	Conference	✓
11	Shared Line Group (SLG)	✓
12	Shared Line Appearance (SLA) or Call Delegation	✓
13	Call Recording	✓
14	Call Flip	✓

Legend

✓	Supported
✗	Not Supported
N/A	Not Applicable

Caveats

Note the following items in relation to this Interop:

- Potential issue has been observed on SBC 5400 for long duration calls (HOLD/UNHOLD from PSTN after 30mins) where SBC management tends to go down. The fix for this issue is available in SBC release 9.2 and beyond. We recommend to use SBC 9.2 release.

Support

For any support related queries about this guide, please contact your local Ribbon representative, or use the details below:

- Sales and Support: 1-833-742-2661
- Other Queries: 1-877-412-8867
- Website: <https://ribboncommunications.com/about-us>

References

For detailed information about Ribbon products & solutions, please visit:

<https://ribboncommunications.com/products>

For detailed information about Zoom products & solutions, please visit:

<https://zoom.us/>

Conclusion

This Interoperability Guide describes a successful configuration covering Zoom interop involving the SBC Core. All the necessary features and serviceability aspects stand covered as per the details provided in this interoperability document.

