Ribbon SBC Edge R11.0 Interop with Zoom Phone Local Survivability : Interoperability Guide

Table of Contents

Interoperable Vendors

Copyright

Document Overview

This document outlines the configuration best practices for the Ribbon solution covering the Ribbon SBC Edge when deployed with Zoom Phone Local Survivability (ZPLS).

About Ribbon SBC Edge

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 SBC Edge (SBC 1000/2000) addresses the next-generation needs of SIP communications by delivering embedded media transcoding, robust security, and advanced call routing in a high-performance, small form-factor device enabling service providers and enterprises to quickly and securely enhance their network by implementing services like SIP Trunking, secure Unified Communications and Voice over IP (VoIP).

The SBC Edge provides a reliable, scalable platform for IP interconnect to deliver security, session control, bandwidth management, advanced media services and integrated billing/reporting tools in an SBC appliance. This versatile series of SBCs can be deployed as peering SBCs, access SBCs or enterprise SBCs (eSBCs). The SBC product family is tested for interoperability and performance against a variety of third-party products and call flow configurations in the customer networks.

⚠ SBC 1000 and SBC 2000 are represented as SBC Edge in the subsequent sections.

About Zoom Phone Local Survivability (ZPLS)

Zoom Phone is a cloud-based service that is dependent on IP connectivity to Zoom’s datacenters. Customers that are using the Zoom Phone solution at corporate locations are encouraged to deploy redundant and reliable internet connectivity with sufficient bandwidth at each corporate office as a base requirement.

For certain business locations maintaining telephony service in the event of an outage is critical. Zoom can offer a survivability solution of basic telephony services in order to provide an additional layer of protection to ensure business continuity. An outage can be the result of an internet service failure at a business location or a failure in multiple Zoom datacenters that prevent client devices from reaching Zoom Phone components.

The Zoom Phone Local Survivability (ZPLS) module leverages the platform and Operating System (OS) provided by the Zoom Node and is distributed as a Linux-based appliance that is spun up on an on-premises VMware ESXi host. The ZPLS module does not affect the phone service during normal operations. Phone clients and devices in survivable Phone Sites register to the corresponding ZPLS module and are able to maintain a subset of Phone features when connectivity to Zoom Phone is lost. When connectivity to the Zoom Phone cloud returns, clients and devices re-register back to the cloud. During the outage, neither the administrator nor the end user is required to take any action to enable survivability. The failover and fallback process is seamless and automatic.

The interoperability compliance testing focuses on verifying inbound and outbound call flows between the Ribbon SBC Edge & ZPLS.

This guide contains the following configuration sections:

- Section A: Ribbon SBC Edge Configuration
  - Captures general SBC Edge configurations for deploying SBC with ZPLS.
- Section B: Zoom Phone Local Survivability Configuration
  - Captures the Zoom Phone Local Survivability configuration.

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.

To perform this interop, you need to:

- use the graphical user interface (GUI) or command line interface (CLI) of the Ribbon product.
- understand the basic concepts of TCP/UDP/TLS and IP/Routing.
- have SIP/RTP/SRTP to complete the configuration and for 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.

Prerequisites

The following aspects are required before proceeding with the interop:

- Ribbon SBC Edge
- Public IP Addresses
- Zoom Go account - a special type of account where the Zoom user can be configured for ZPLS.
- TLS Certificates for Ribbon SBC Edge signed by one of the Zoom approved CA vendors.

Product and Device Details

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

Table 1: Requirements

	Appliance/Application/Tool	Software Version
Ribbon Communications	SBC 2000	11.0.1 build 634
Zoom	Zoom Phone Local Survivability (ZPLS)	1.8.0.73
	Zoom Client	5.11.10 (8200)
PSTN Phone	Jitsi	2.10.5550
Administration and Debugging Tools	Ribbon LX Tool	2.1.0.6

Note

- ZPLS version is 1.8.0.73 or later.
- Zoom Client version is 5.11.10 (8200) or later.
- Jitsi version is 2.10.5550 or later.

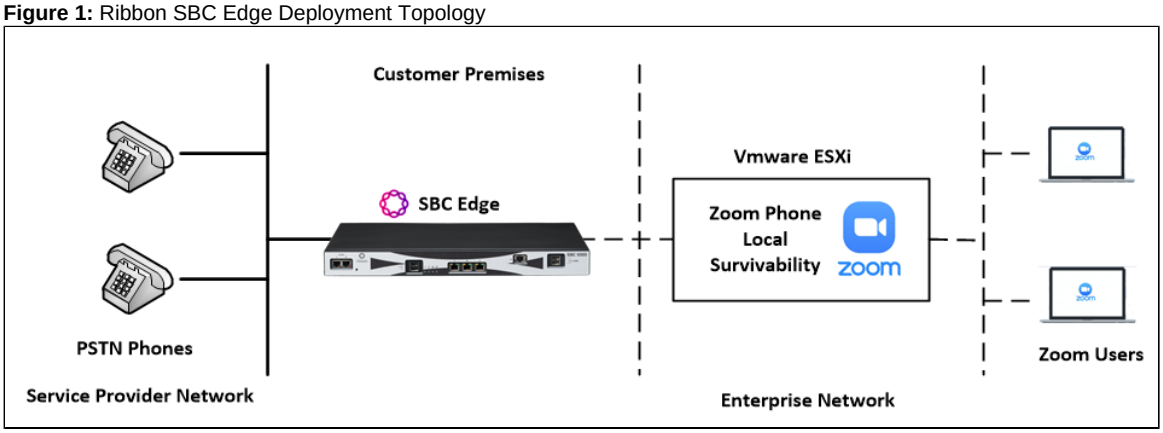
Network Topology Diagram

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

Deployment Topology : Geographically Located

This deployment topology depicts the ZPLS on a host server which is geographically different from the SBC Edge location.

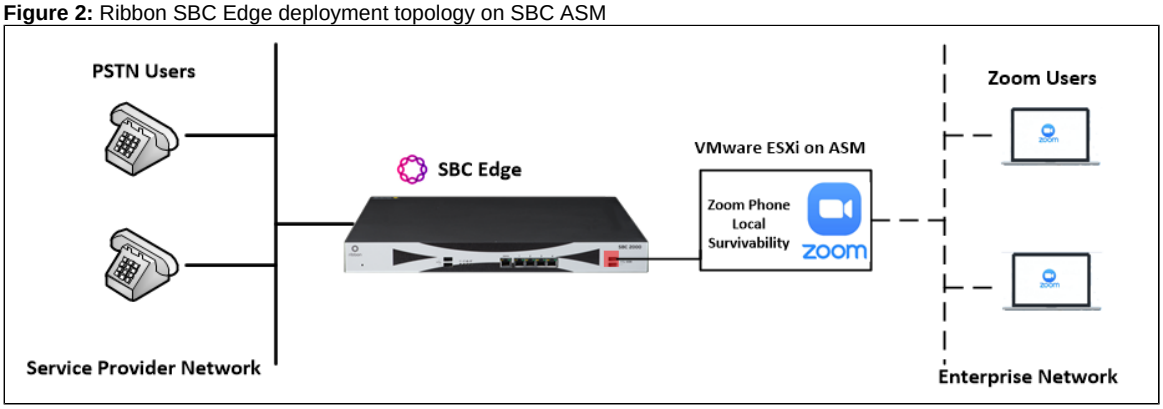
Figure 1: Ribbon SBC Edge Deployment Topology



Deployment Topology : Co-located & Centralized

This deployment topology depicts ZPLS installed as VM on ASM (Application Solution Module) within the SBC Edge 1K/2K platform.

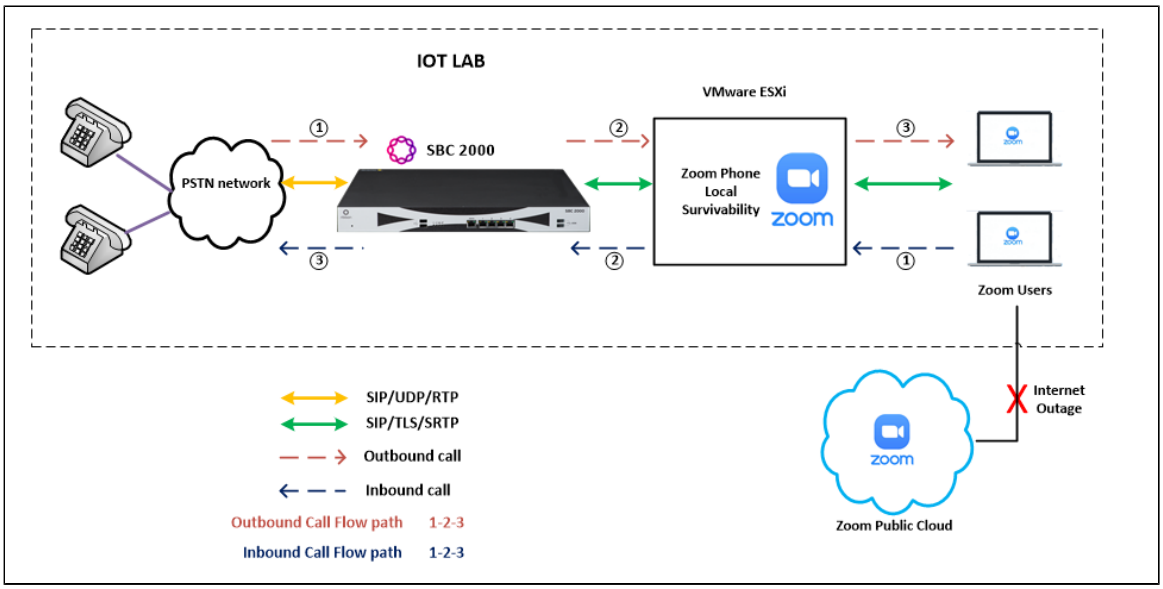
Figure 2: Ribbon SBC Edge deployment topology on SBC ASM



Interoperability Lab Topology : Geographically Located

The following lab topology diagram shows connectivity between the Ribbon SBC Edge on a virtual platform and Zoom Phone Local Survivability.

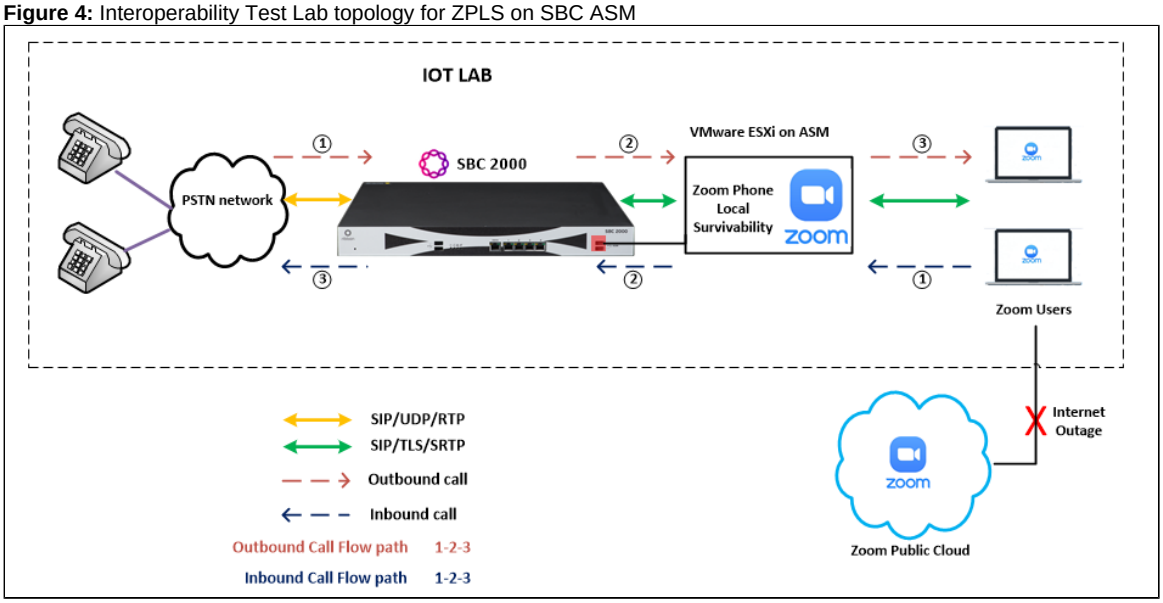
Figure 3: SBC Edge and ZPLS interoperability Test Lab Topology



Interoperability Lab Topology : Co-located & Centralized

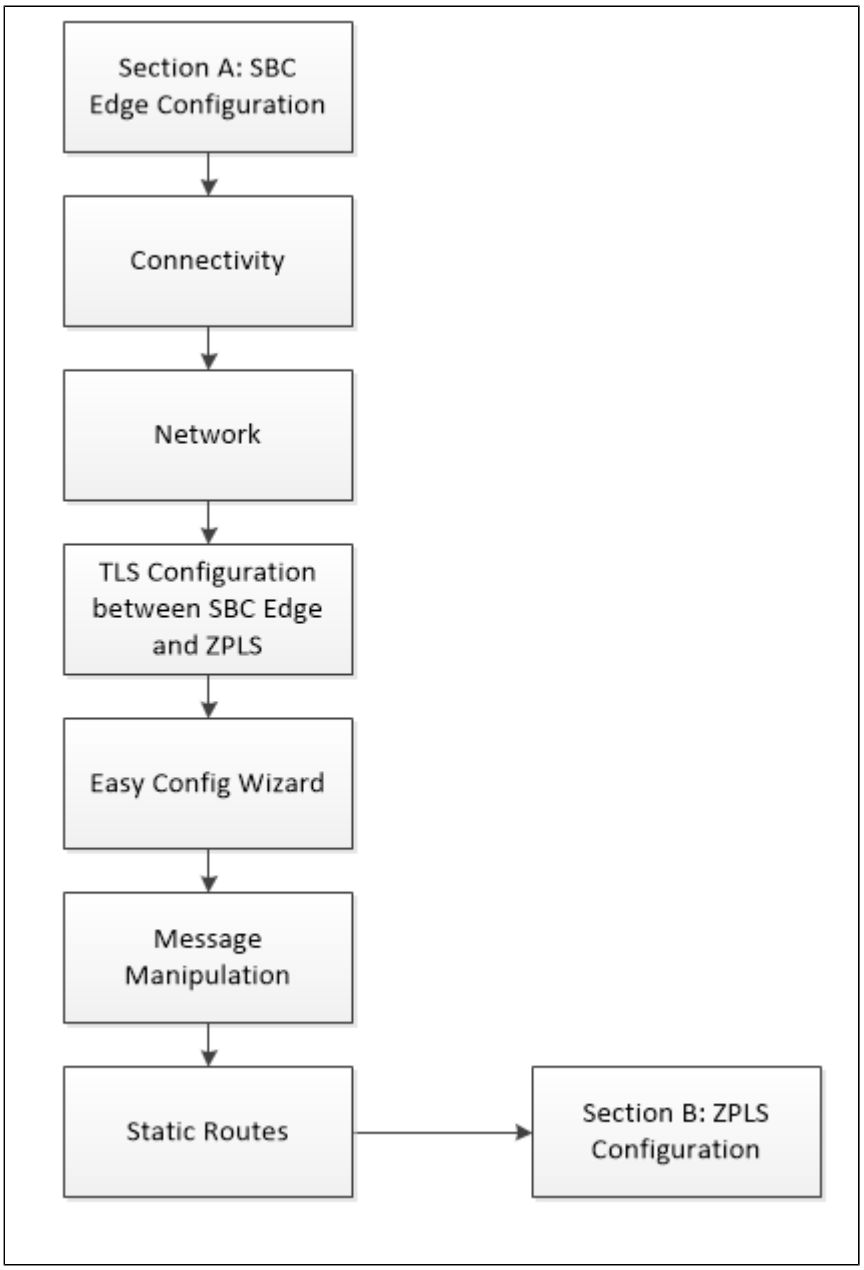
The following lab topology diagram shows connectivity between Ribbon SBC Edge and Zoom Phone Local Survivability on SBC's ASM (Application Solution Module).

Figure 4: Interoperability Test Lab topology for ZPLS on SBC ASM



Document Workflow

The sections in this document follow the sequence below. The reader is advised to complete each section for successful configuration.



- For Deployment Topology : Co-located & Centralized - Follow Section C: Install VMware ESXi on SBC ASM to install VMware ESXi on ASM.
- Remaining SBC configuration would remain same as mentioned in the document workflow.

Section A: Ribbon SBC Edge Configuration

The following SBC Edge configurations are included in this section:

Connectivity

Network

Static Routes

TLS Configuration between SBC Edge and ZPLS

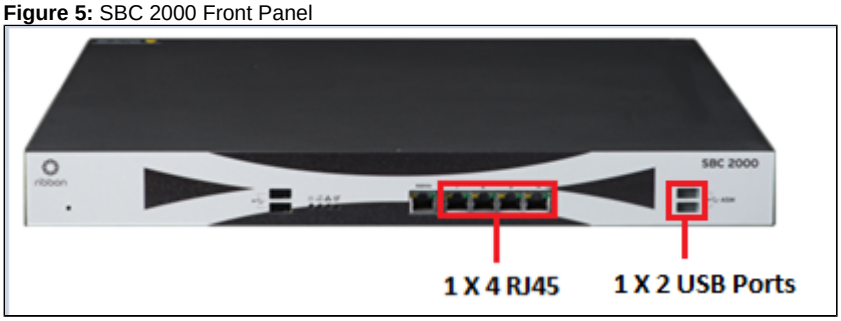
Easy Config Wizard

Message Manipulation

- SBC Edge can connect to the network as mentioned in Connectivity and Network.
- Zoom prefers transport as TLS. Establishing a TLS connection between SBC Edge and ZPLS is covered under TLS Configuration between Ribbon SBC Edge and ZPLS.
- Configure the SBC Edge with PSTN and ZPLS using Easy Config Wizard.

Connectivity

Figure 5: SBC 2000 Front Panel



SBC 2000 is connected to the network as follows:

Ethernet 1: RJ45 "1" is connected towards the PSTN leg.

Ethernet 2: RJ45 "2" is connected towards the ZPLS leg.

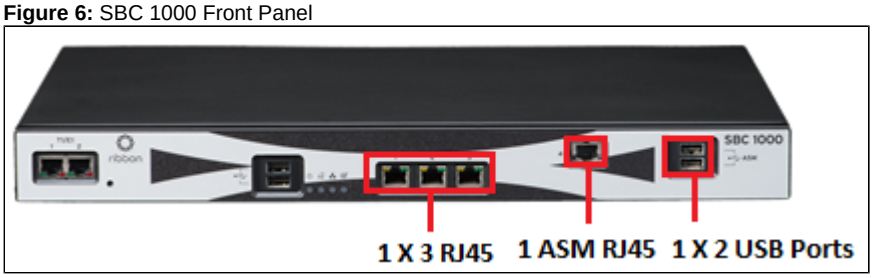
USB 1: USB - LAN adapter used to connect ASM to network.

USB 2: Connect the keyboard.

Deployment Topology : Co-located & Centralized would make use of the USB ports to connect to the network. USB-LAN adapter would be required to connect ASM to network on SBC 2000.

SBC 1000 has a dedicated ASM port to connect to enterprise network.

Figure 6: SBC 1000 Front Panel



SBC 1000 is connected to the network as follows:

Ethernet 1: RJ45 "1" is connected towards the PSTN leg.

Ethernet 2: RJ45 "2" is connected towards the ZPLS leg.

ASM port: RJ45 "1" is connected to enterprise network.

USB 2: Connect the keyboard.

Network

Configure Ethernet 1 and Ethernet 2 of SBC 1000/2000 with the IP as follows:

Navigate to **Node Interfaces > Logical Interfaces.**

Figure 7: Logical Interfaces

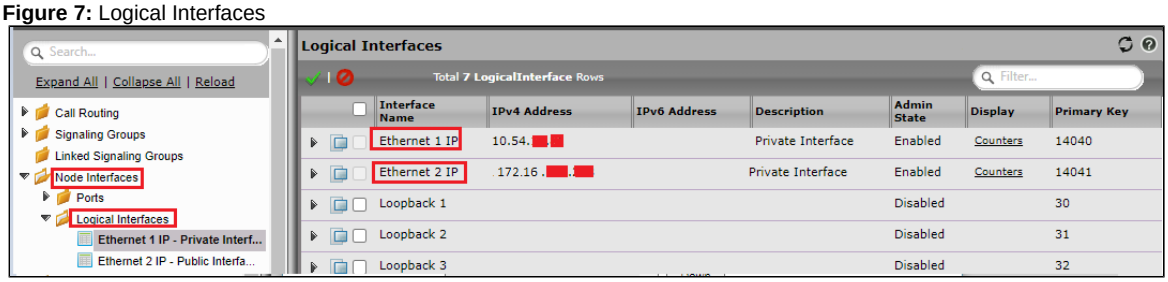
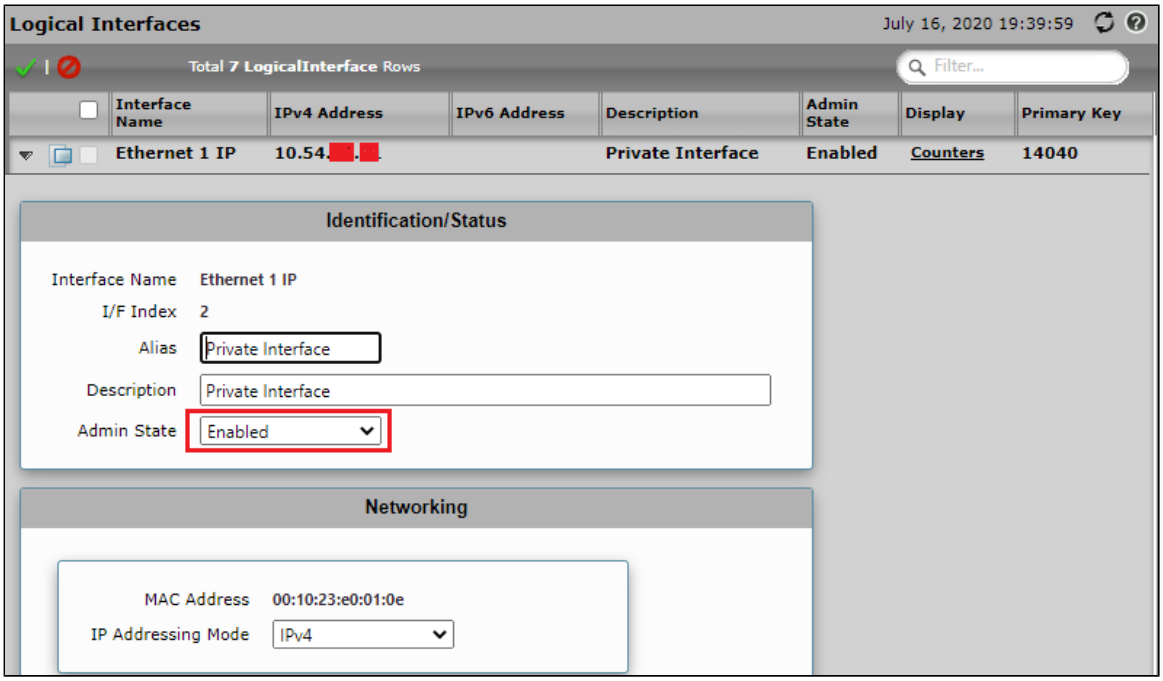


Figure 8: Ethernet 1



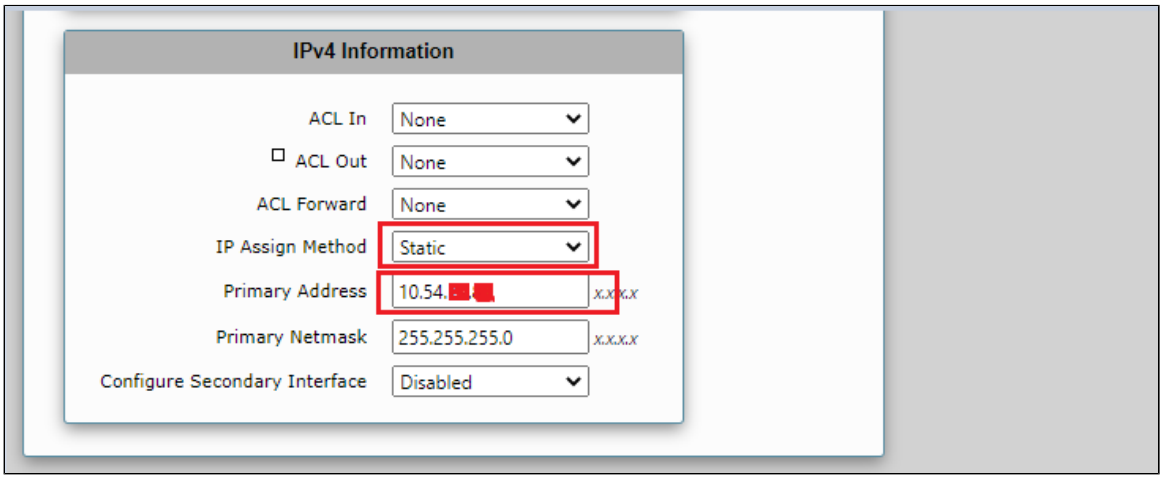
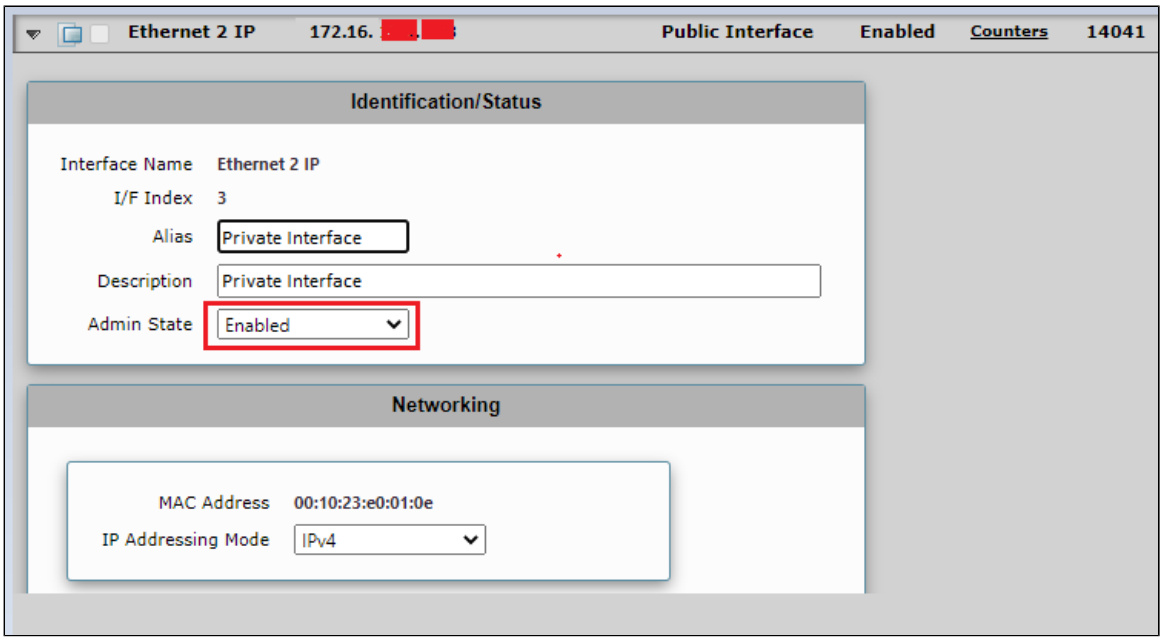
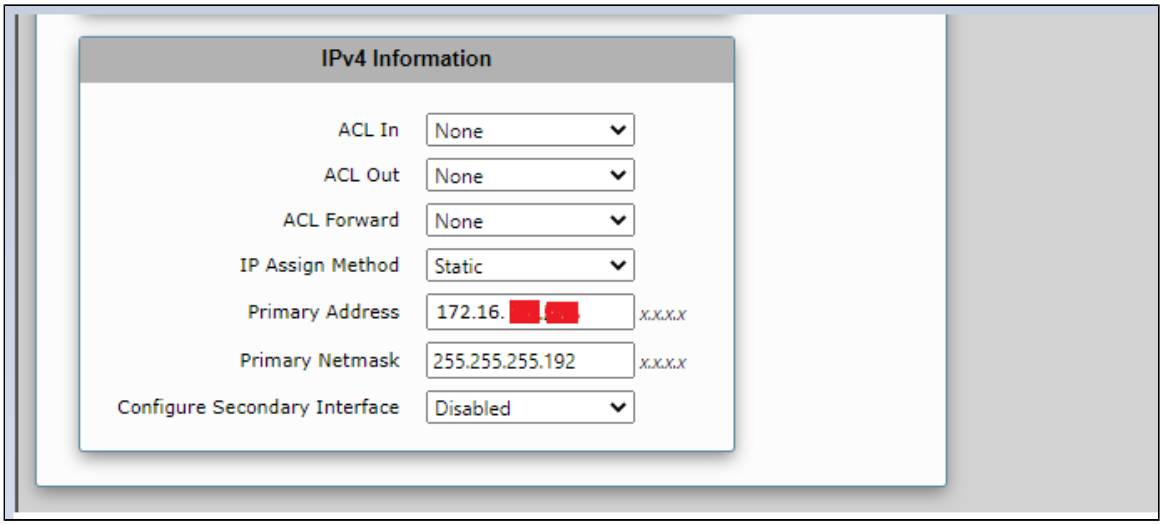


Figure 9: Ethernet 2





Tip
To configure Ethernet 1 and Ethernet 2 of SBC SWe Edge, navigate to **Networking Interfaces > Logical Interfaces.**

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

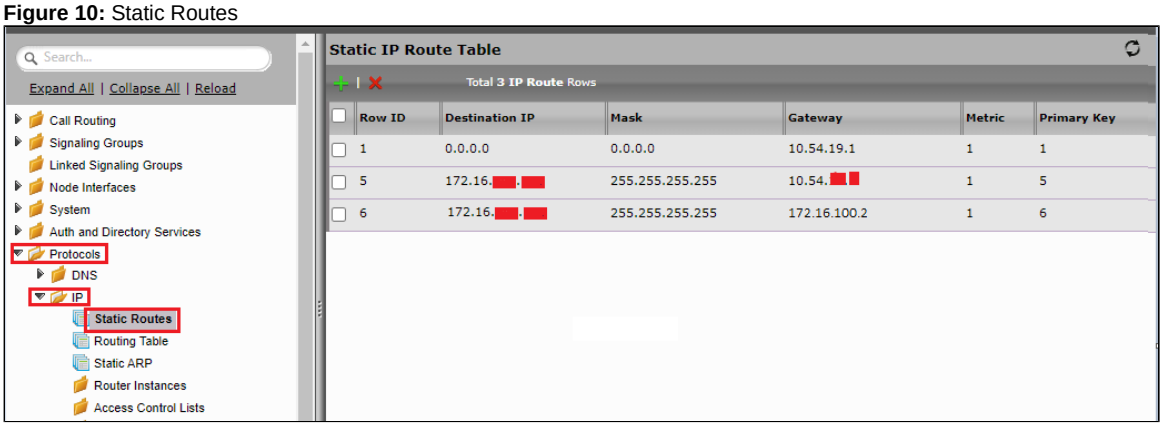
- For smaller networks with just one or two routes, configuring static routing is preferable. This is often more efficient since a link is not being wasted by exchanging dynamic routing information.
- For networks that have a LAN-side Gateway on Voice VLAN or Multi-Switch Edge Devices (MSEs) with Voice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

Static routes need to be added towards the Eth1 interface 172.16.X.X (PSTN) and the Eth2 interface 172.16.X.X (ZPLS).

Default static route is towards the Eth1, which is in a private network.

- Navigate to **Settings > Protocol > IP > Static Routes** to configure the routes.

Figure 10: Static Routes



TLS Configuration between SBC Edge and ZPLS

Prerequisites:

- For TLS to work on the public side of the network, a trusted Certificate Authority (CA) is needed. In this scenario, GoDaddy is used as a trusted CA.
- Digicert Global Root CA and Digicert Global G2 are also required for TLS handshake.
- ZPLS is enabled with TLS/SRTP by default.

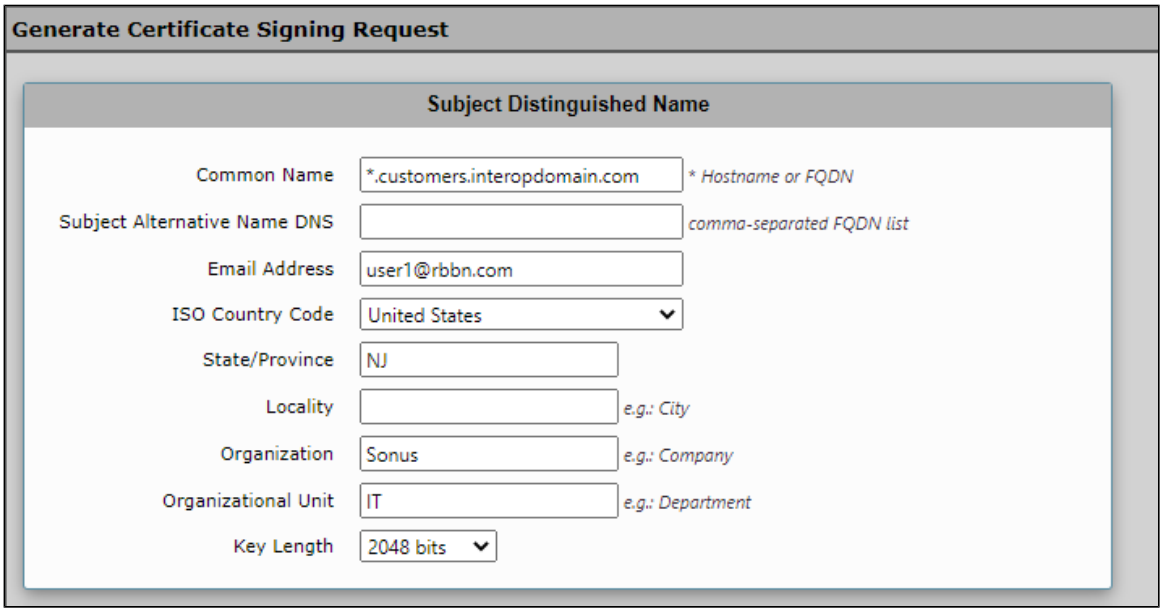
Request a certificate for the SBC and configure it based on the example using GoDaddy as follows:

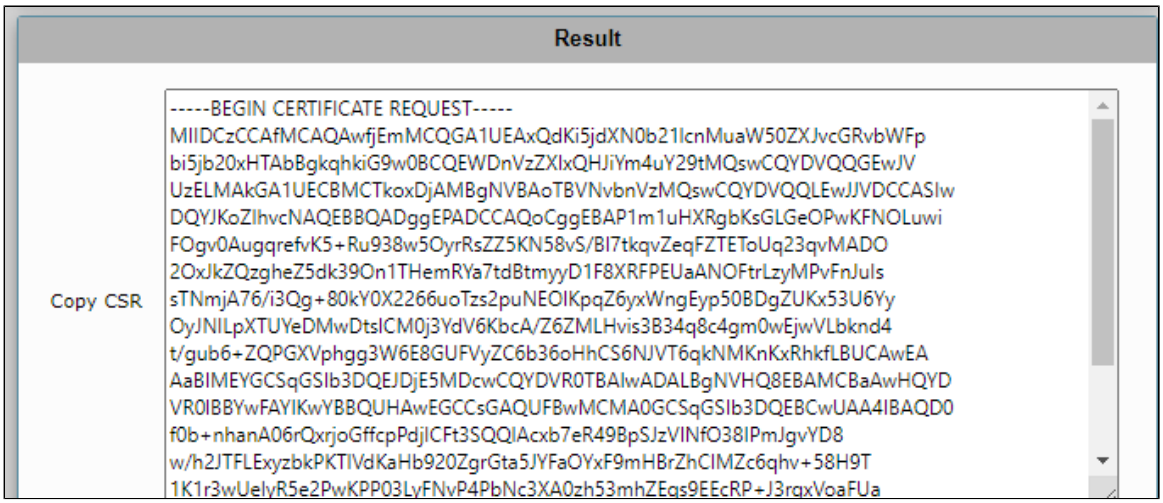
- Generate a Certificate Signing Request (CSR) and obtain the certificate from a Certificate Authority.
- Import the Public CA Root/Intermediate Certificate and the SBC Certificate on the SBC.

Step 1: Generate a Certificate Signing Request and obtain the certificate from a Certificate Authority (CA).

- Navigate to **Settings > Security > SBC Certificates.**
- Click **Generate SBC Edge CSR.**
- Enter data in the required fields. Click **OK**. After the Certificate Signing Request is generated, copy the result to the clipboard.
- Use the generated CSR text from the clipboard to obtain the certificate.

Figure 11: Generate Certificate Signing Request





Step 2: Deploy the Root/Intermediate and SBC certificates on the SBC.

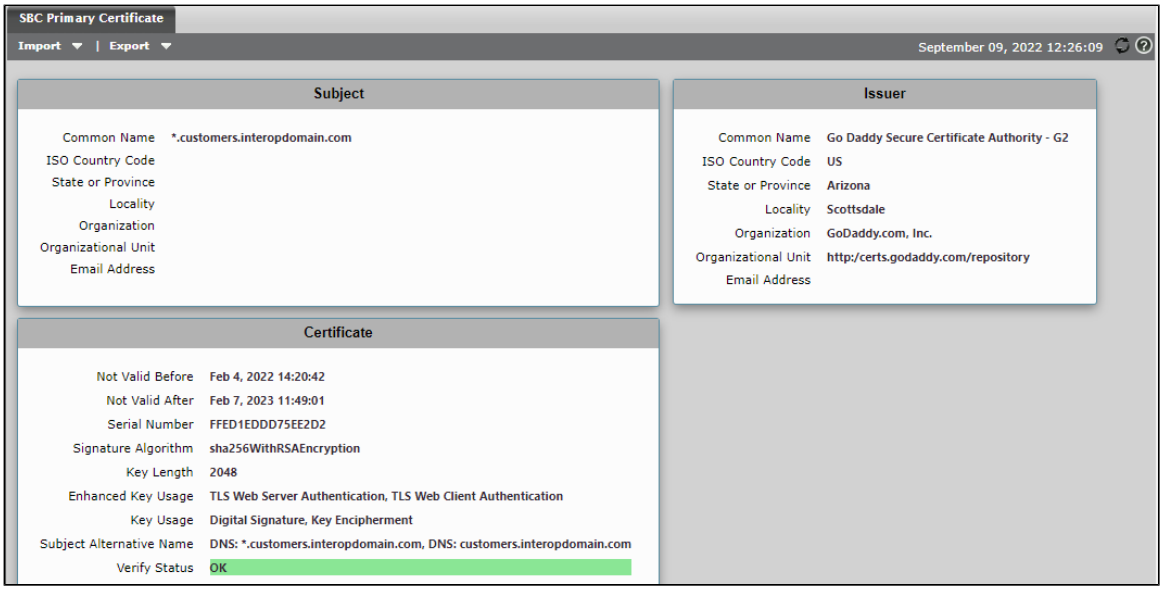
After receiving the certificates from the certificate authority, install the SBC Certificate and the Root/Intermediate certificates as follows:

- Obtain Trusted Root and Intermediary signing certificates from your Certificate Authority.
- To install the Trusted Root/Intermediate certificates, go to **Settings > Security > SBC Certificates > Trusted Root Certificates.**
- Click **Import** and select the trusted root certificates.
- To install the SBC certificate, open **Settings > Security > SBC Certificates > SBC Edge Certificate.**
- Validate the certificate is installed correctly.

Figure 12: Trusted CA certificate table

- Click **Import** and select **X.509 Signed Certificate.**
- Validate the certificate is installed correctly.

Figure 13: Validate certificate

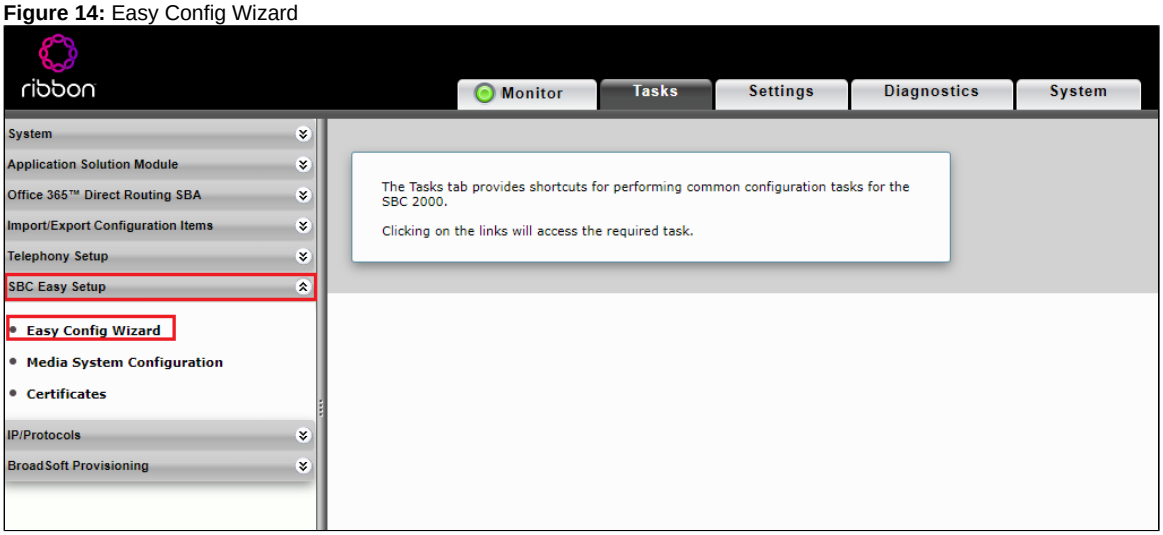


Easy Config Wizard

Configure the SBC Edge with ZPLS using the Easy Config Wizard.

- Access the WebUI of SBC 2000.
- Click on the **Tasks** tab.
- From the left side menu, click **SBC Easy Setup > Easy Config Wizard.**

Figure 14: Easy Config Wizard

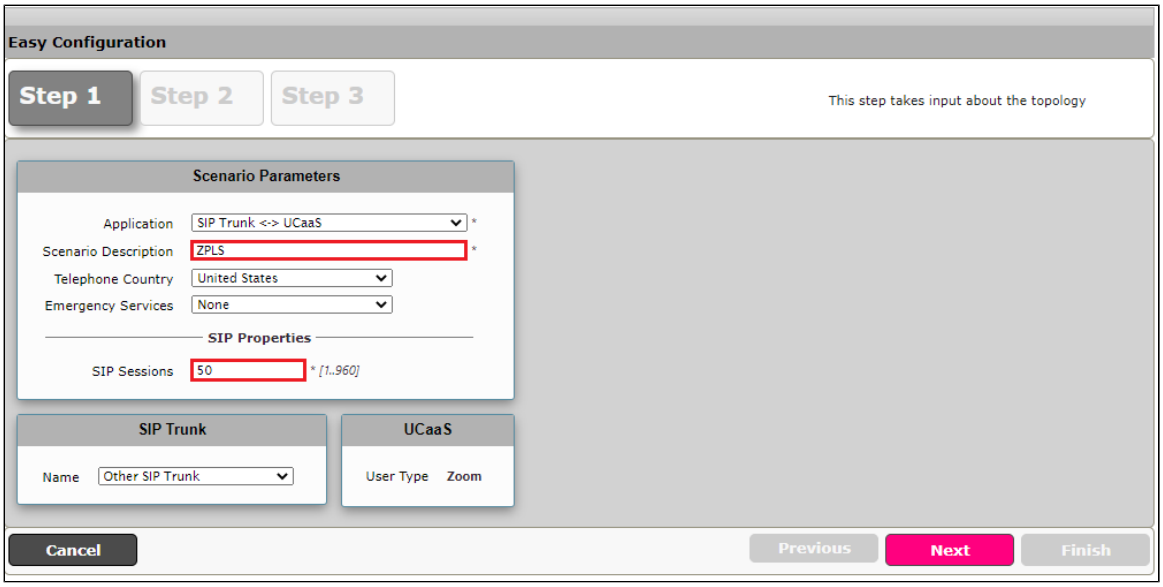


Fill in the details for Step 1 as follows:

- Scenario Description as **ZPLS**.
- SIP Sessions as **50**.

> Enter a value for SIP sessions as per the requirement. The value can be up to 960.

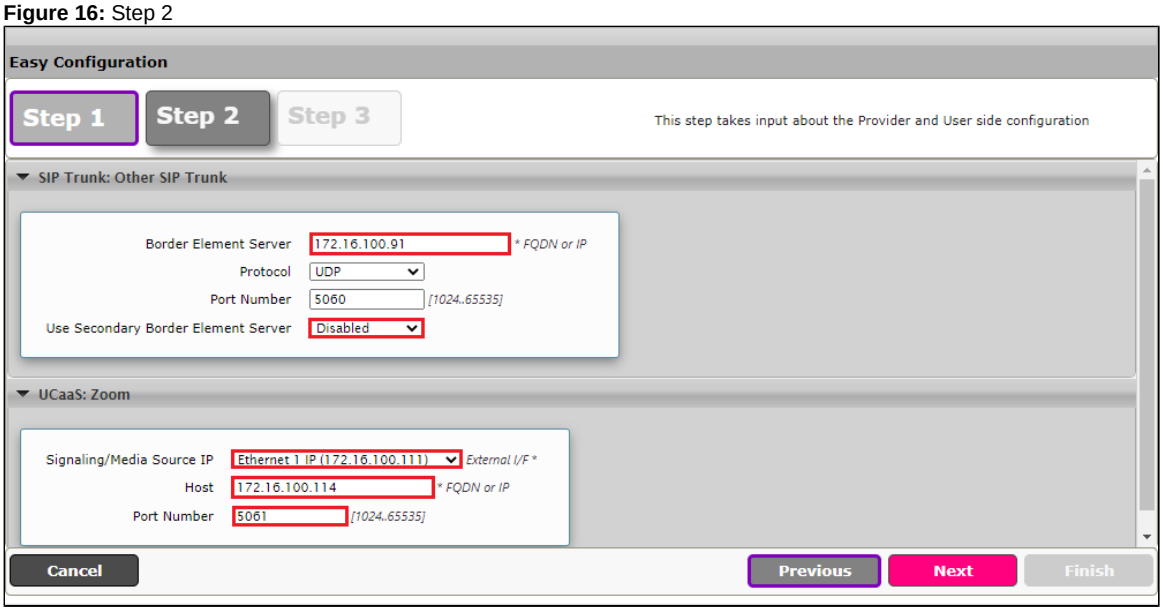
Figure 15: Step 1



Fill in the details for Step 2 as follows:

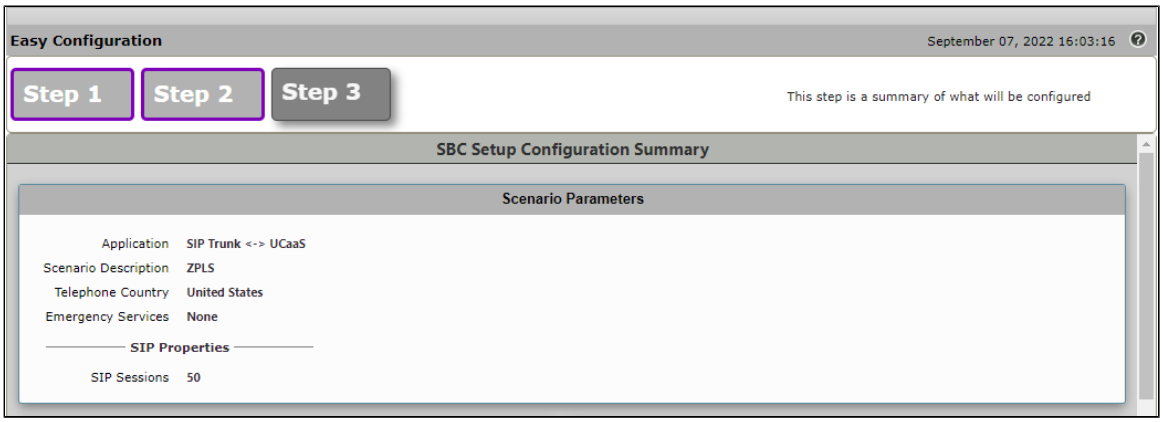
- Border Element Server would be the PSTN IP.
- Use Secondary Border Element Server should be **Disabled**.
- Signaling/Media Source IP towards ZPLS.
- Host IP of the ZPLS.
- Port of the ZPLS, i.e. 5061.

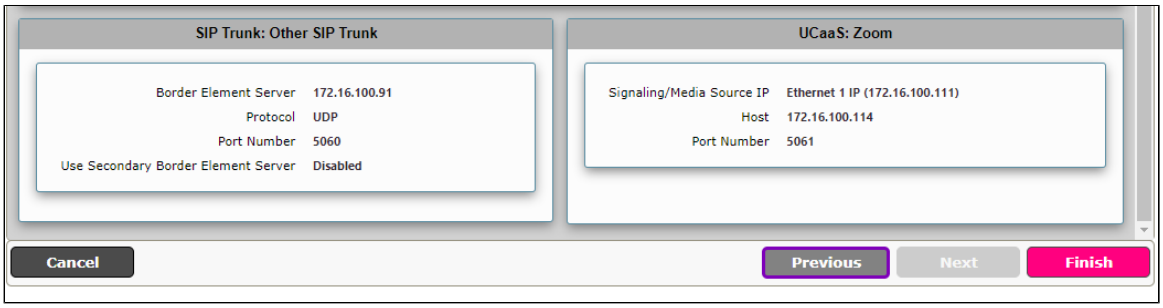
Figure 16: Step 2



Review the configurations in Step1 and Step 2, and click on the **Finish** button.

Figure 17: Step 3





Message Manipulation

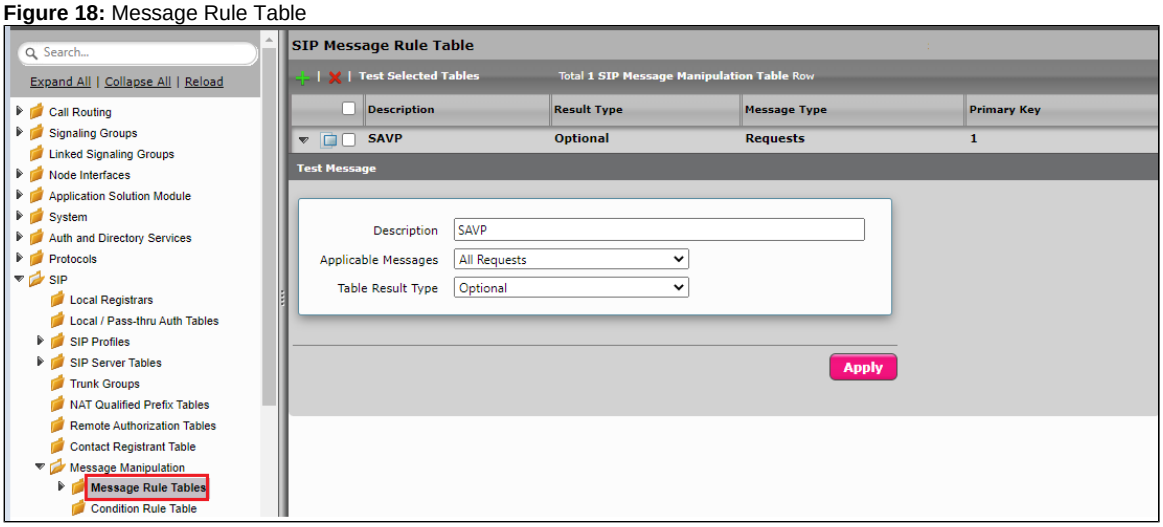
The Message Manipulation SAVP is used for the following purposes:

- To modify the RTP/AVP to RTP/SAVP for all the request messages.

Go to **Settings** > **SIP** > **Message Manipulation** >**Message Rule Tables.** Click the + icon to create a Message Rule Table.

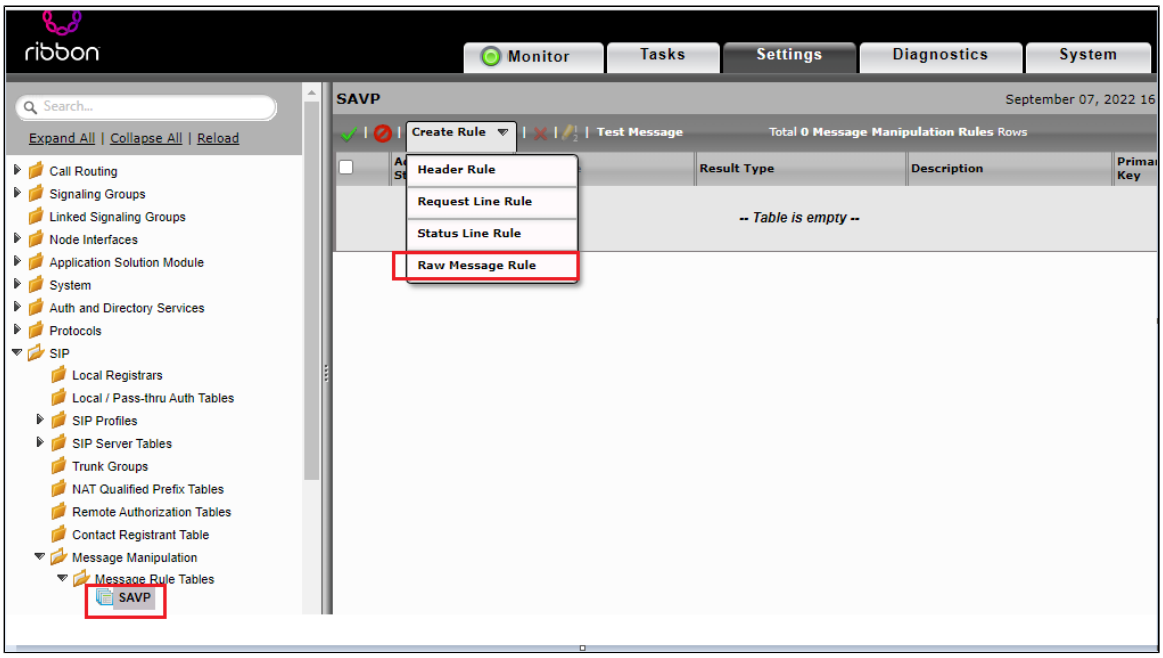
- Provide a description for the Rule Table.
- Apply Message Rule to "All Requests".
- Click OK.

Figure 18: Message Rule Table



Create **Raw Message Rule** as follows:

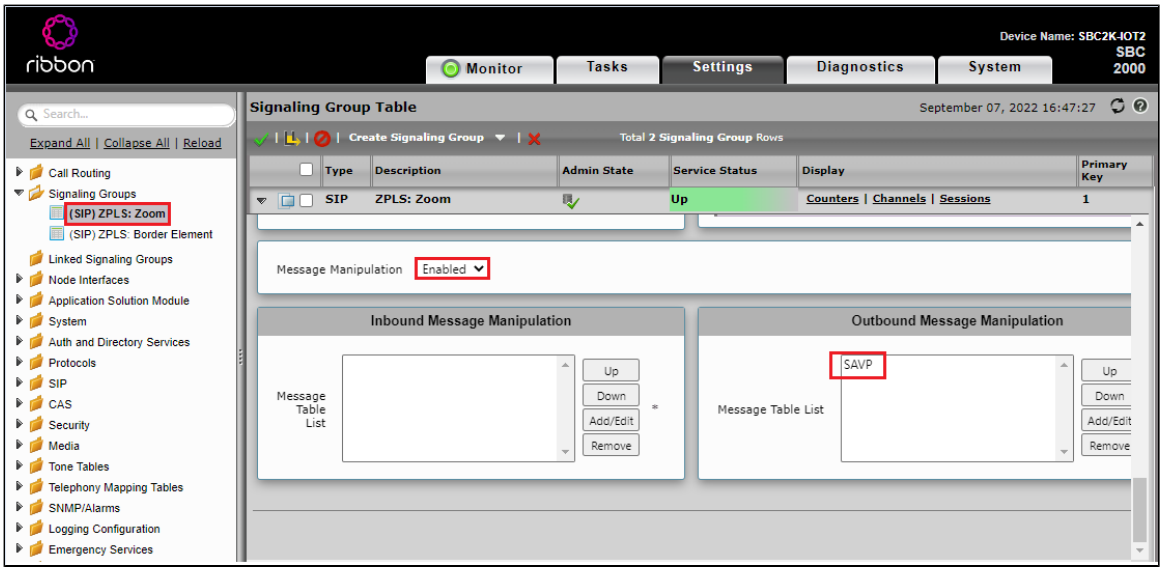
Figure 19: Raw Message Rule



Go to the **Signaling Groups > (SIP) ZPLS:Zoom** as created earlier with Easy Config Wizard.

Apply the Outbound Message Manipulation rule to the Zoom Signaling Group as shown below.

Figure 20: Message Manipulation



Section B: Zoom Phone Local Survivability Configuration

For configuring both Zoom Phone System and Zoom Phone Local Survivability, refer to the following link:

https://support.zoom.us/hc/en-us/articles/360001297663-Getting-started-with-Zoom-Phone-admin.

Section C: Install VMware ESXi on SBC ASM

SBC 2000 Chassis

Install VMware ESXi & USB-LAN driver (to convert USB port to ethernet port) in order to connect the ASM to the network using the following steps:

- Download VMware ESXi 7.0 licensed version along with the USB-LAN converter driver.
- For more information regarding VMware ESXi, refer to:
  https://customerconnect.vmware.com/web/vmware/evalcenter?p=free-esxi6

- For more information regarding USB-LAN converter driver, refer to:
  https://flings.vmware.com/usb-network-native-driver-for-esxi?download_url=https%3A%2F%2Fdownload3.vmware.com%2Fsoftware%2Fvmw-tools%2FUSBNND%2FESXi670-VMKUSB-NIC-FLING-39203948-offline_bundle-16780994.zip#instructions

- Remove the front cover of SBC 2000 chassis
  - Locate the mini-VGA port and connect the matching plug of proprietary cable.
  - Connect the the other end (VGA plug) to to the monitor.
- Insert the bootable USB pen drive (with VMware ESXi 7.0 image) to one of the ports of "USB hub".
- Connect the keyboard to another USB Port.
- Insert the "USB to LAN" converter adaptor (Dongle) to the bottom USB Port (on the right side of the equipment written as "ASM") to convert the USB port to an ethernet port.
- Insert an ethernet cable to the "USB to LAN" converter adaptor and connect the other end to the LAN switch (network).
- Configure the hostname according to the unique serial number of the box.
- Power off and then Power on the equipment to reboot and detect the bootable USB drive.
- Select 'boot' from bootable USB drive to start the VMware installation.
  - Follow the instructions prompted by VMware installation process to install VMware ESXi 7.0 on the ASM till VMware installation is complete.
  - Once the VMware ESXi installation completes, enable SSH by logging in via a web browser.
  - Next, go to Host manage services TSM-SSH Start.
- Upload the USB to the LAN converter driver file "ESXi670-VMKUSB-NIC-FLING-39203948-offline_bundle-16780994.zip" to the VMware ESXi host under the /tmp/ folder.
- Using puTTY, ssh to the VMware server and enter credentials to log in,
- Use the command below to install:

```
[root@localhost:/tmp] esxcli software vib install -d /tmp/ESXi670-VMKUSB-NIC-FLING-39203948-offline_bundle-
16780994.zip

Installation Result

   Message: The update completed successfully, but the system needs to be rebooted for the changes to be
effective.

   Reboot Required: true

   VIBs Installed: VMW_bootbank_vmkusb-nic-fling_2.1-6vmw.670.2.48.39203948

   VIBs Removed:

   VIBs Skipped:

[root@localhost:/tmp]
```

- At the prompt, enter "reboot**"** and press **Enter**.

SBC 1000 Chassis

Install VMware ESXi and connect the ASM's only ethernet port to the network

- Download VMware ESXi 7.0 licensed version.
- For more information regarding VMware ESXi, please refer the link https://customerconnect.vmware.com/web/vmware/evalcenter?p=free-esxi6.
- Copy the downloaded licensed VMware ESXi 7.0 iso image to a USB pendrive and make it bootable drive.
- Insert the bootable USB pendrive with VMware ESXi 7.0 image to top USB port on the right side of the equipment marked as "ASM".
- Insert the keyboard to another USB port on the right side of the equipment marked as "ASM".
- Insert the ethernet cable to "ethernet" port on the right side of the equipment marked as "ASM" and connect other end of ethernet cable to the LAN switch.
- Follow the instructions to install VMware ESXi 7.0 on the ASM.

Once the VMware ESXi is installed on ASM, continue with Section A: Ribbon SBC Edge Configuration for further configurations.

Supplementary Services and 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	Internal Extension Dialing	✓
2	Dial By Name	✓
3	Dial From Call History	✓
4	OPTIONS ping (SBC to ZPLS)	✓
5	OPTIONS ping (ZPLS to SBC)	✓
6	Basic Call from PSTN to Zoom	✓
7	Basic Call from Zoom to PSTN	✓
8	Call Hold & Call Resume	✓
9	Mute/Unmute	✓
10	DTMF (RFC 2833)	✓

11	Blind/Unattended Transfer	✓
12	Consultative/Attended Transfer	✓
13	Call Park & Retrieve	✓
14	Adhoc 3-Party Conference	✓

Legend

✓	Supported
✗	Not Supported
N/A	Not Applicable

Caveats

The following items should be noted in relation to this Interop - these are either limitations, untested elements, or useful information pertaining to the Interoperability.

- SBC Edge Media List created using Easy Config Wizard would have the G711-Alaw as highest priority then G711-Mulaw. Alter the codec priority as per requirement.

Support

For any support related queries about this guide, 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/services/ribbon-support-portal

References

For detailed information about Ribbon products & solutions, go to :

https://ribboncommunications.com/products

For information about Zoom products & solutions, go to:

https://zoom.us

Conclusion

This Interoperability Guide describes a successful configuration of the Zoom Phone Local Survivability interoperability with Ribbon SBC Edge.

All features and capabilities tested are detailed within this document - any limitations, notes or observations are also recorded in order to provide the reader with an accurate understanding of what has been covered, and what has not.

Configuration guidance is provided to enable the reader to replicate the same base setup - there maybe additional configuration changes required to suit the exact deployment environment.