Deployment Guide

AudioCodes Professional Services

Mediant™ 800C SBC with Zoom Phone Local Survivability

zoomphone

audiocodes

Notice

Date Published: November-22-2023

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our website at https://www.audiocodes.com/services-support/maintenance-and-support.

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our website at https://online.audiocodes.com/documentation-feedback.

Stay in the Loop with AudioCodes

Related Documentation

Document Name
Mediant 800 Gateway & E-SBC User's Manual
SIP Message Manipulation Reference Guide
AudioCodes Configuration Notes

Document Revision Record

LTRT	Description
29372	Initial document release.
29375	TLS Private Key size of 1024 was removed. Minor typo fixes.
29376	Prerequisites section added; note added re Zoom support of wildcard certificate.
29377	Zoom Node GUI updates; new password policy.
29401	New Zoom trusted public certificates.

Table of Contents

1 Introduction

This document provides step-by-step instructions on installing and configuring the Zoom Phone Local Survivability (hereafter, referred to as *ZPLS*) module running on AudioCodes Mediant 800C Session Border Controller (hereafter, referred to as *SBC*).

About the Zoom Phone Local Survivability

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 some business locations, maintaining telephony service in the event of an outage is critical. Zoom can offer a survivability solution of basic telephony services 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 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 can 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.

For more details about ZPLS, refer to the Zoom Help Center.

About AudioCodes SBC Product Series

AudioCodes' family of SBC devices enables reliable connectivity and security between Enterprise's and the service provider's VoIP networks.

The SBC provides perimeter defense as a way of protecting Enterprises from malicious VoIP attacks; mediation for allowing the connection of any PBX and/or IP-PBX to any service provider; and Service Assurance for service quality and manageability.

Designed as a cost-effective appliance, the SBC is based on field-proven VoIP and network services with a native host processor, allowing the creation of purpose-built multiservice appliances, providing smooth connectivity to cloud services, with integrated quality of service, SLA monitoring, security, and manageability. The native implementation of SBC provides a host of additional capabilities that are not possible with standalone SBC appliances such as VoIP mediation, PSTN access survivability, and third-party value-added services applications. This enables Enterprises to utilize the advantages of converged networks and eliminate the need for standalone appliances.

AudioCodes SBC is available as an integrated solution running on top of its field-proven Mediant Media Gateway and Multi-Service Business Router platforms, or as a software-only solution for deployment with third-party hardware. The SBC can be offered as a Virtualized SBC, supporting the following platforms: Hyper-V, AWP, KVM, VMware, AWS, Azure and GCP.

2 Environment Information

This section describes the typical deployment environment.

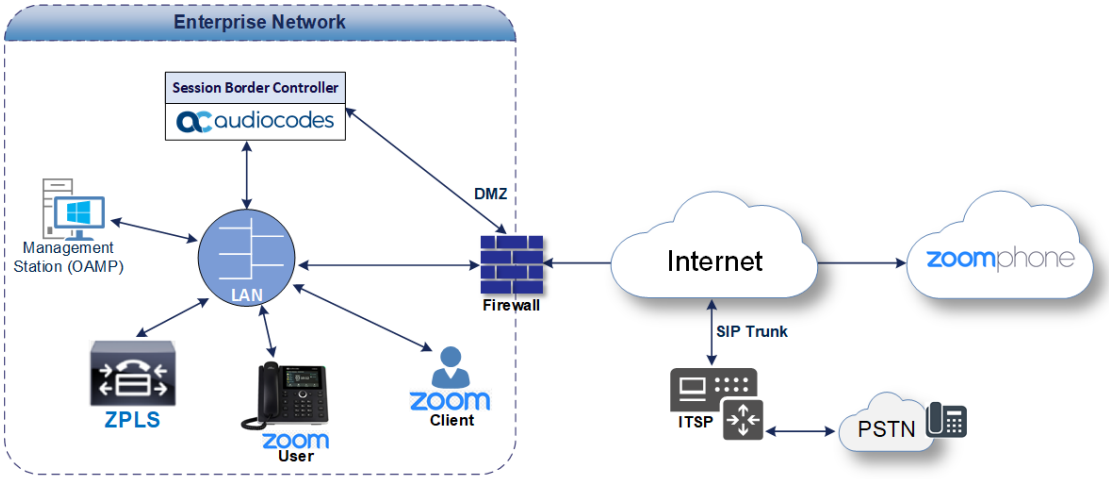
Deployment Topology

The interoperability between AudioCodes SBC and ZPLS with the Generic SIP Trunk and Zoom Phone system done using the following topology setup:

- ZPLS module pre-installed on the integrated Open Solutions Network (OSN) server of the Mediant 800C device and connected to the enterprise LAN.
- Enterprise connected with the Zoom Phone System located on the WAN for enhanced communication within the Enterprise.
- Enterprise wishes to offer its employees enterprise-voice capabilities and to connect the Enterprise to the PSTN network in case of Zoom Phone System connectivity outage using AudioCodes SIP Trunking service.
- AudioCodes SBC is implemented to interconnect between the ZPLS module, SIP Trunk and the Zoom Phone System.
  - **Session:** Real-time voice session using the IP-based Session Initiation Protocol (SIP).
  - **Border:** IP-to-IP network border. The ZPLS module is located in the Enterprise LAN. The AudioCodes SBC, SIP Trunk and Zoom Phone System are located in the public network.

The following figure illustrates this deployment topology:

Figure 2-1: Layout of Typical Deployment Environment



Environment Setup

The typical deployment topology includes the following environment setup:

Table 2-1: Environment Setup

Area	Setup
Network	■ ZPLS module is located on the LAN. ■ Both, Zoom Phone System and Generic SIP Trunk environments are located on the WAN.
Signaling Transcoding	■ Both Zoom Phone systems (ZPLS and Cloud) operates with SIP-over-TLS transport type. ■ Generic SIP Trunk can operate with SIP-over-UDP or SIP-over-TCP or SIP-over-TLS transport type (depends on particular provider).
Codecs Transcoding	■ Both Zoom Phone systems support OPUS, G.711A-law, G.711U-law and G.729 coders. ■ Generic SIP Trunk supports G.711A-law, G.711U-law, and G.729 coders (or other coders, depending on the requirement).
Media Transcoding	■ Both Zoom Phone systems operate with SRTP media type. ■ Generic SIP Trunk operates with RTP media type.

3 Safety Precautions

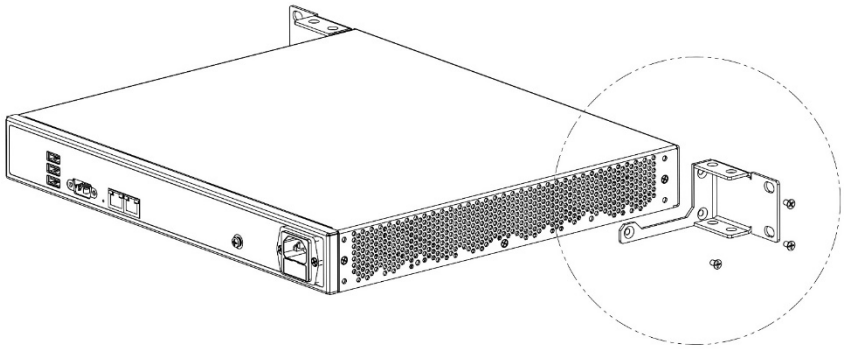
- AudioCodes Mediant 800C device is an indoor unit and therefore must not be installed outdoors. Ethernet cabling must be routed only indoors and must not exit the building.
- The device must be installed and serviced only by qualified service personnel.
- Do not open or dismantle the device.
- Do not expose the device to water or moisture.
- Make sure the device is installed in a well-ventilated location to avoid overheating of internal components and subsequent damage.
- Do not place any object on top of the device and make sure that sufficient clearance from the top and sides are maintained to ensure proper airflow to avoid over heating of internal components.
- Operate the device in an ambient temperature (Tma) that does not exceed 40°C (104°F).
- The device must be installed only in restricted access locations.
- Use only the supplied AC power cord for connection to the power source.
- The device must be connected to an electrical socket-outlet providing a protective earthing connection.
- Operate the device only from the type of power source indicated on the chassis.
- Installation of the device must be in accordance with national wiring codes and conform to local regulations.
- The device must be installed only in telecommunication sites in compliance with ETS 300-253 requirements "Earthing and Bonding of Telecommunication Equipment in Telecommunication Centers".
- Prior to installation, earth loop impedance test must be performed by a certified electrician to ensure grounding suitability at the power outlet intended to feed the device. It's essential that impedance is kept below 0.5 ohms.

4 Mounting the Device

The device offers the following mounting options:

- Desktop mounting, using the four anti-slide rubber feet (supplied), which you need to stick on the grooves located on the underside of the device.
- Wall mounting, using side-mounting brackets (separate orderable item).
- Standard 19-inch rack mounting, by placing it on a pre-installed rack shelf (not supplied), and secure it to the rack frame using the front-mounting brackets (supplied).

Figure 4-1: Mounting AudioCodes Mediant 800C device



5 Connecting Device to Power

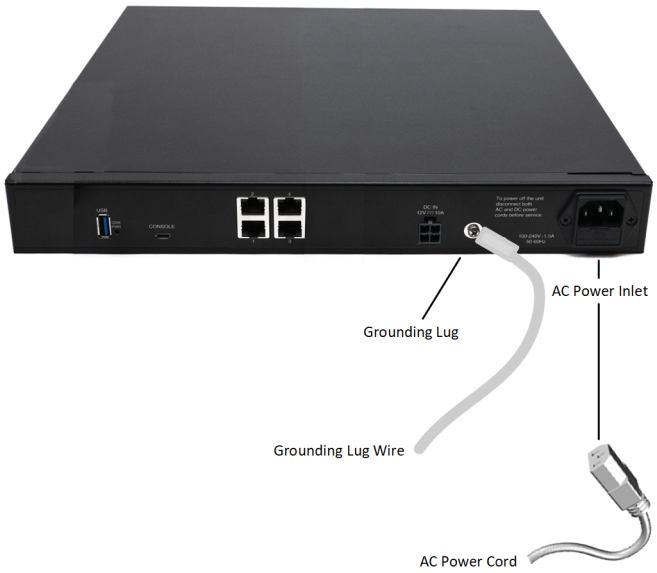
The device is powered from a standard alternating current (AC) electrical wall outlet.

Warning (Grounding): The device must always be grounded (earthed). Grounding should be done in accordance with the safety and electrical regulations enforced in the country of installation.

➢ **To connect device to power:**

1. Ground the device, by connecting an electrically earthed strap of 16-AWG wire (minimum) to the device's grounding screw (located on the rear panel), using the supplied washer and fasten the wire securely using a 6-32 UNC screw. Connect the other end of the strap to protective earthing.
2. Connect the device to power by plugging the AC power cord (supplied) into the device's AC power inlet, located on the rear panel. Connect the plug at the other end of the AC power cord to a standard AC electrical wall outlet.
3. Check that the device is receiving power (**POWER** LED on front panel should be on - green).

Figure 5-1: Connecting AudioCodes Mediant 800C device to the power



6 Configuring Zoom Phone Local Survivability Module

AudioCodes Mediant 800C device is supplied with Zoom Phone Node pre-installed on its integrated Open Solutions Network (OSN) server. This section describes configuration of the ZPLS service only.

In case of disaster recovery of the Zoom Phone Node, see Recovering ZPLS from Disaster on page 61.

The following steps need to be done for activating the ZPLS service:

- Configuring and starting Zoom Node virtual machine pre-installed on the integrated Open Solutions Network (OSN) server of the Mediant 800C device.
- Setup ZPLS module.
- Assign SBC to the ZPLS module.

Prerequisites

Before you begin:

- Make sure that your Zoom account has Zoom Node Monthly / Annual and Zoom Phone Hybrid subscriptions, and Local Survivability Service is enabled. Contact your Zoom account team for assistance.
- Make sure that you have Zoom Portal owner or admin credentials with appropriated privileges (e.g., to manage Zoom Node).
- Make sure that Local Survivability Mode is enabled in your Zoom account:
  a. Sign-in to the Zoom web portal at https://zoom.us.
  b. In the Navigation menu, click **Account Management**.
  c. Click **Account Settings**.
  d. Under **Zoom Phone**, check that the **Local Survivability Mode** is enabled.
- Make sure that Multiple Sites functionality is enabled for your Zoom account:
  a. Sign-in to the Zoom web portal at https://zoom.us.
  b. In the Navigation menu, click **Phone System Management**, and then click **Company Info**.
  c. Click **Account Settings**.
  d. Under **Settings**, check that **Multiple Sites** is enabled.
- Review the Zoom Node firewall documentation and make sure that your firewall allows communication to the destination addresses through the required ports.

- If HTTPS Proxy is implemented in your network, make sure to add the URL ***.digicert.com** to the whitelist of the HTTPS Proxy.

Zoom Node Configuration

This section describes how to configure and register the Zoom Node, pre-installed on AudioCodes Mediant 800C's OSN module.

Make sure that the VMware server is licensed.

Changing VMware Host's Network Settings

This section describes how to configure network settings (IP address, default gateway, DNS, etc.) of the VMware host machine, pre-installed on the AudioCodes Mediant 800C's OSN module.

AudioCodes Mediant 800C's OSN module is supplied with 5 Ethernet NICs, 4 external (located on the rear panel of the Mediant 800C) and one internal NIC for interconnect between OSN module and SBC. By default, network connectivity to the ZPLS application is available via 'vnic' (ported to external Ethernet port #1). Meaning, the Mediant 800C should be connected to the network via two separate Ethernet cables: one, on the rear, connects the OSN (for the ZPLS app), and another, on the front, connects to the SBC application.

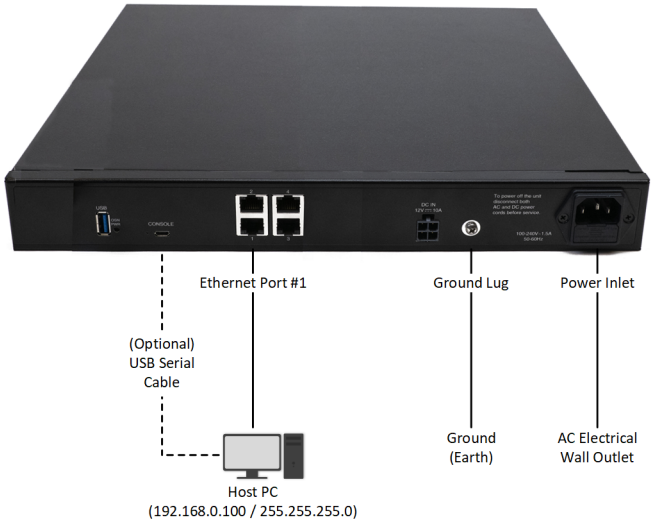
Customers that prefer to connect both the SBC and ZPLS applications to the network via a single Ethernet cable, need to enable the internal vnic (see Enabling OSN's Internal vNIC on page 73 for detailed instructions).

The default IP address of the VMware ESXi host on whose virtual machine the ZPLS module is running is 192.168.0.10/24. You can change this address (and other network settings) to suit your IP addressing scheme.

➢ **To change VMware host's networking address:**

1. Connect the RJ-45 connector on one end of the Ethernet cable to the device's Gigabit Ethernet port #1 (located on the rear panel), and then connect the other end of the cable to your computer (or laptop).

Figure 6-1: Connecting AudioCodes Mediant 800C device to the network

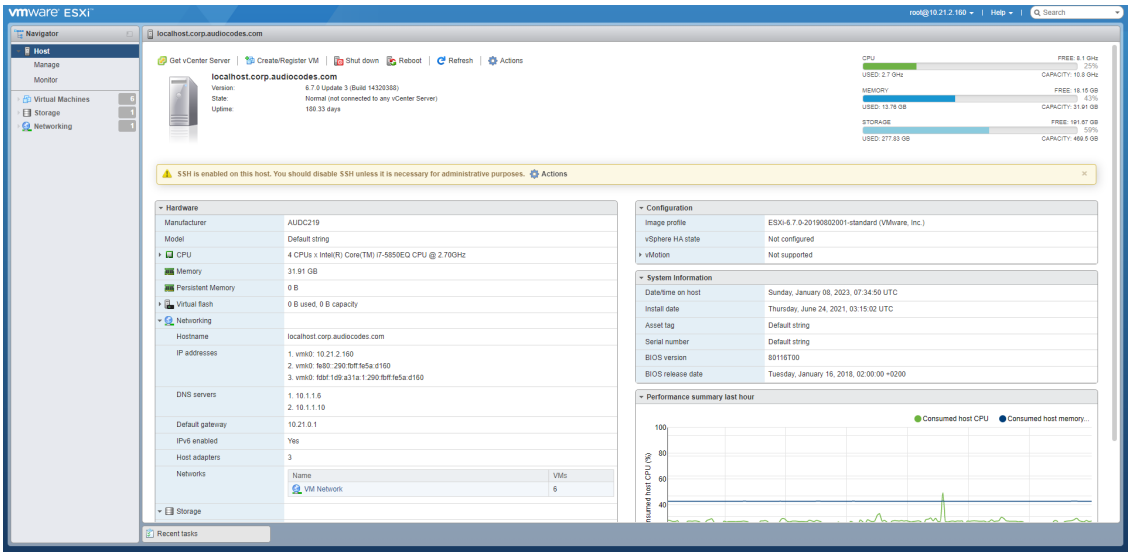


2. Change your computer's IP address (e.g., 192.168.0.100/24) so that it's in the same subnet as the default address of the VMware host.
3. On your computer, open any Web browser, and then browse to URL address 192.168.0.10; the VMware host's login screen appears:

4. Enter the default login credentials:
   - Username: **root**
   - Password: **Audc1234@**

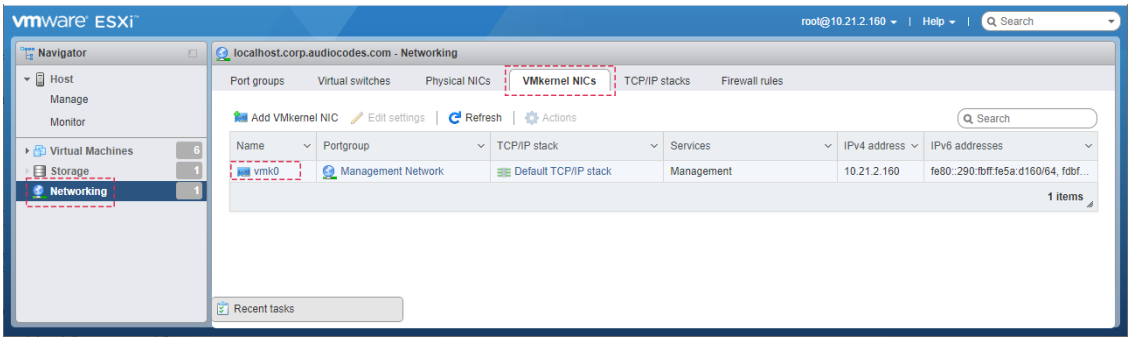
> The root password might be **silicom123!** for some devices.

5. Click **Log in**; the VMWare ESXi Web-based management interface opens:

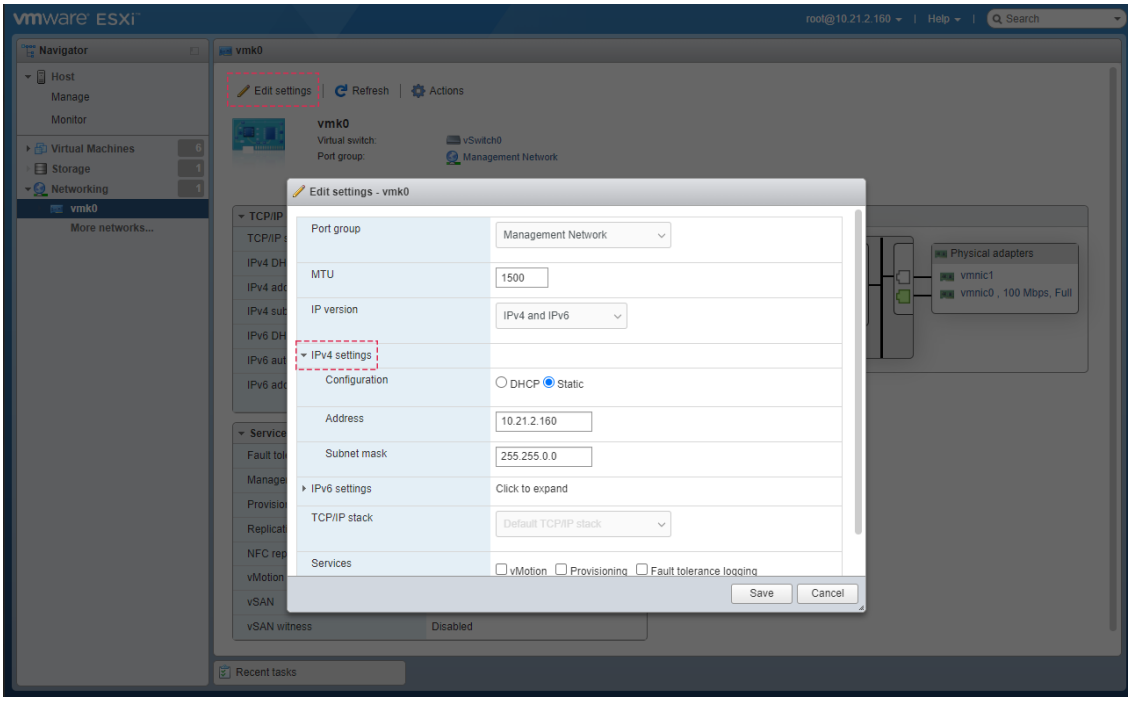


6. In the Navigator pane, click **Virtual Machines**, and then select the "ZPLS" virtual machine.

7. In the Navigator pane, click **Networking**, select the **VMkernel NICs** tab, and then click the "vmk0" NIC:



8. Click **Edit settings**, in the dialog box, expand **IPv4 settings**, and then configure the host's networking address:



9. Click **Save**; you are disconnected from the VMware management interface (because of the changed IP address).
10. Reconnect the device's Ethernet port #1 to your network, and then access the VMware host using the newly assigned IP address.
11. In the Web browser, browse to the newly assigned IP address and log in again to the VMWare ESXi Web-based management interface.
12. In the Navigator pane, click **Networking**, select the **TCP/IP stacks** tab, and then click the "Default TCP/IP stack".
13. Click **Edit settings**, and then in the dialog box, configure the host's IPv4 gateway.
14. Click **Save**.

Configuring Zoom Node Virtual Machine

This section describes the initial configuration of the Zoom Node Virtual Machine.

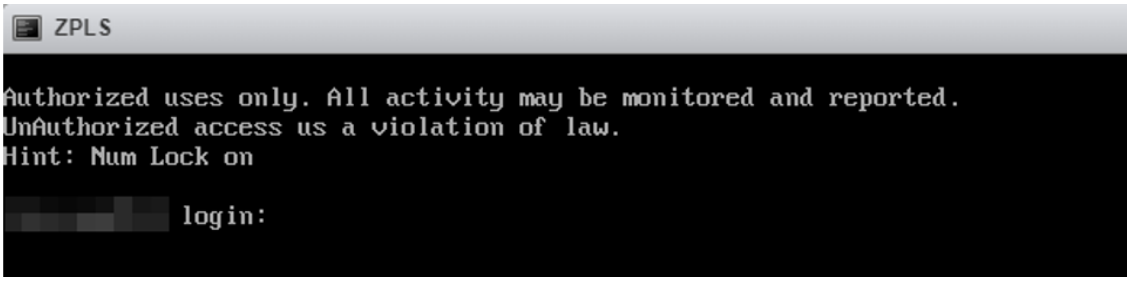
> Information in this section is based on official Zoom Support documentation, which may be updated from time to time by Zoom.

Changing Password for Setup User

After starting Zoom Node Virtual Machine for the first time, you it's recommended that you change the password for the setup user. The setup user name is "zoom-setup". It's necessary for logging in during future use of the Zoom Node text user interface (TUI) console.

➢ To change the password for the setup user:

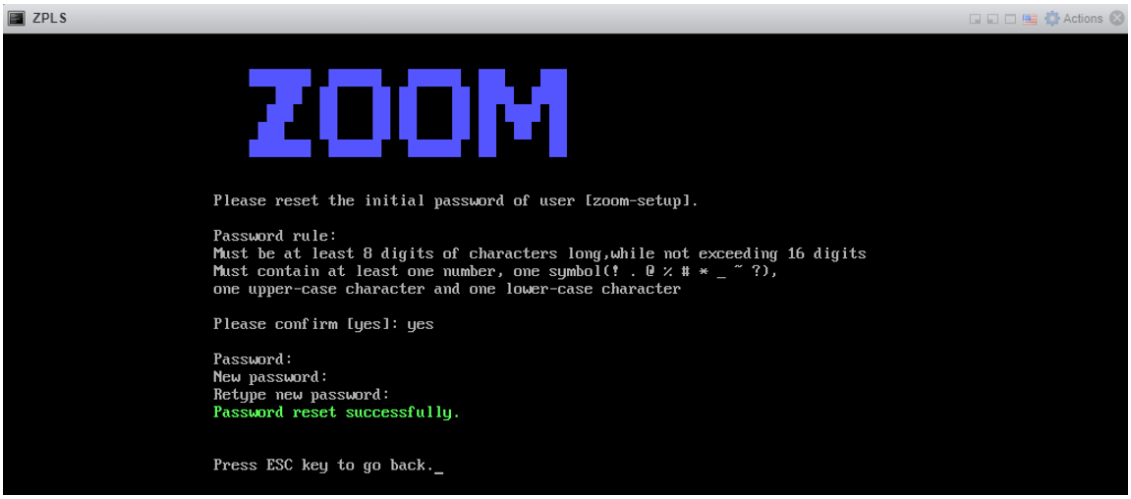
1. Start up the Zoom Node Virtual Machine in vCenter.
2. Access the Zoom Node Virtual Machine TUI console; the following menu appears:



3. Enter the predefined credentials:
   - Username: **zoom-setup**
   - Password: **Audc123#**
4. Press **5** to **Reset Password**.

Currently, exclamation marks (!) and hyphens (-) are not supported for the password.

5. Type **Yes**, and then create a new password for the “zoom-setup” user. Save the password for future use in the TUI console.



6. Once the password has been set, you are prompted to modify the hostname for the Zoom Node server:

7. Enter the desired hostname and domain, and then press the **Enter** key.

Configuring the Zoom Node Network Interface

This section describes how to configure network settings (IP address, default gateway, DNS, etc.) of the Zoom Node server.

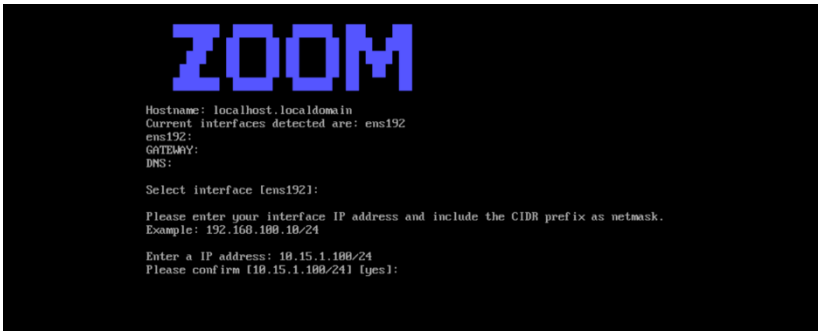
➢ To configure the Zoom Node Network Interface:

1. In the main menu, press **1** to open the network configuration. The following menu is displayed:

2. Save the value for **Current interfaces detected are**, as that is used for the IP address configuration.

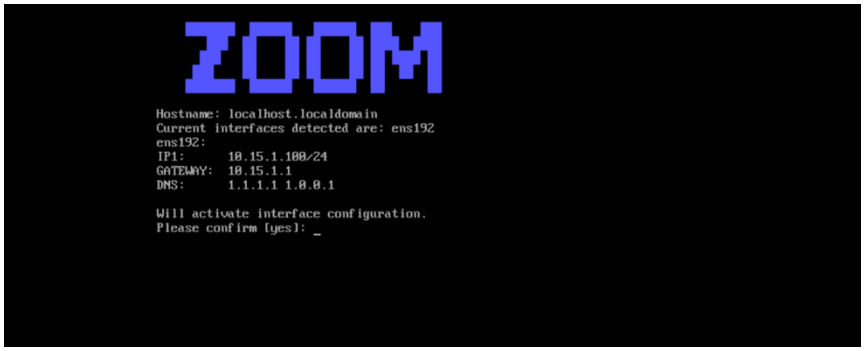
> If Zoom Node is deployed in the network with DHCP enabled, it automatically acquires an address. This address is listed directly below the network interface name, as well as the Gateway and DNS addresses. However, it's highly recommended to use static addresses.

3. Press **1** to add the primary IP address.
4. Press **Enter**, to select the network interface for configuration.
5. Enter the IP address and subnet mask (e.g., 10.15.77.51/16).
6. Press **Enter** to accept the new address and when prompted for confirmation, type **Yes** and press the Enter key. The new IP address is listed with the rest of the network information.



7. Enter the DNS and gateway information for the network interface.

8. Press **Enter** to confirm the new changes.
9. Press **4** to activate the network configuration.



10. Press **Enter** to confirm the new changes.

Removing Addresses Set through DHCP (Optional)

While this is not necessary for configuration, it's recommended to remove any addresses that were automatically assigned if DHCP was utilized and utilize static addresses only.

➢ To remove addresses set through DHCP:

1. In the main menu, press **1** to open the network configuration.
2. Press **2** to access 'Remove an IP address'.
3. Press the **Enter** key to modify the suggested interface or type the name of the desired network interface and press **Enter** to modify it.

4. Type the IP address, and then press **Enter**.
5. Type **YES** to confirm you want to remove the address, and then press **Enter**.

Test Zoom Node Network Connectivity

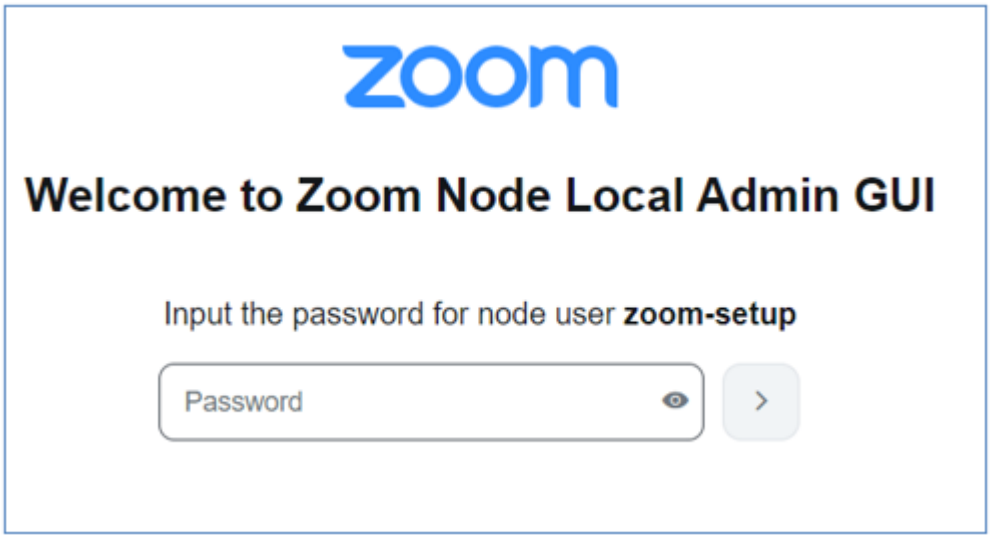
Once the network interfaces have been configured for the Zoom Node Virtual Machine, network connectivity for the Zoom Node Server should be tested to ensure proper function. It's mandatory before registering Zoom Node.

➢ **To test Zoom Node Network Connectivity:**

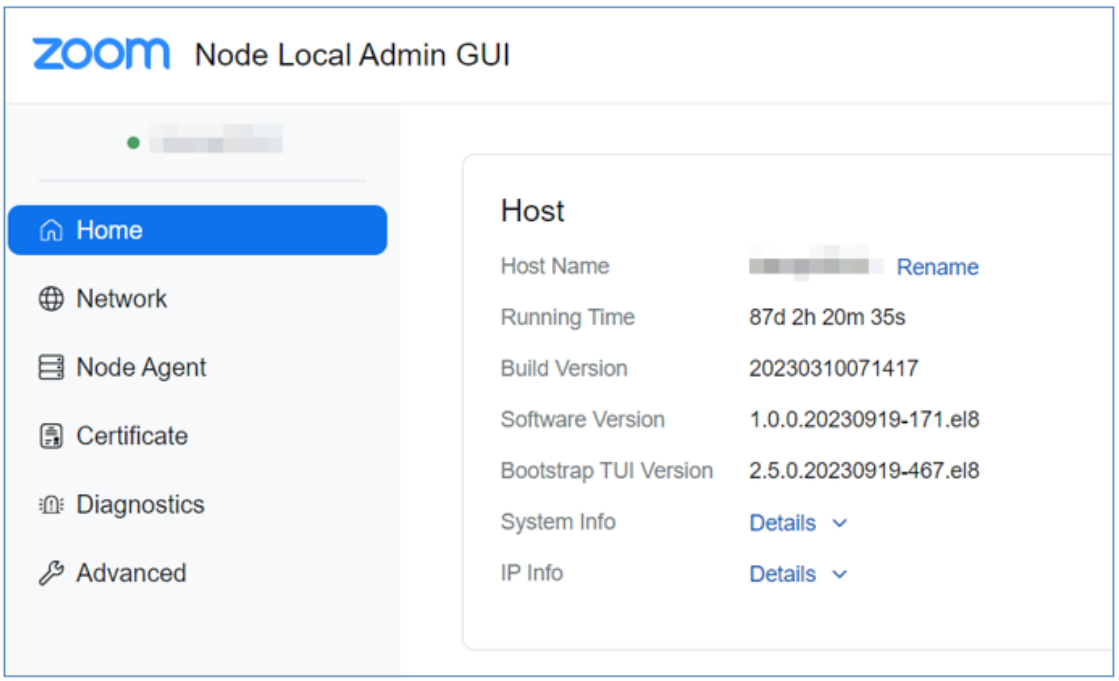
1. Using your web browser, navigate to the Zoom Node web console at https://[IPaddress]:8443, where the IP address is what you configured in Removing Addresses Set through DHCP (Optional) on the previous page.

> If you receive a security warning, accept the warning and continue to the site.

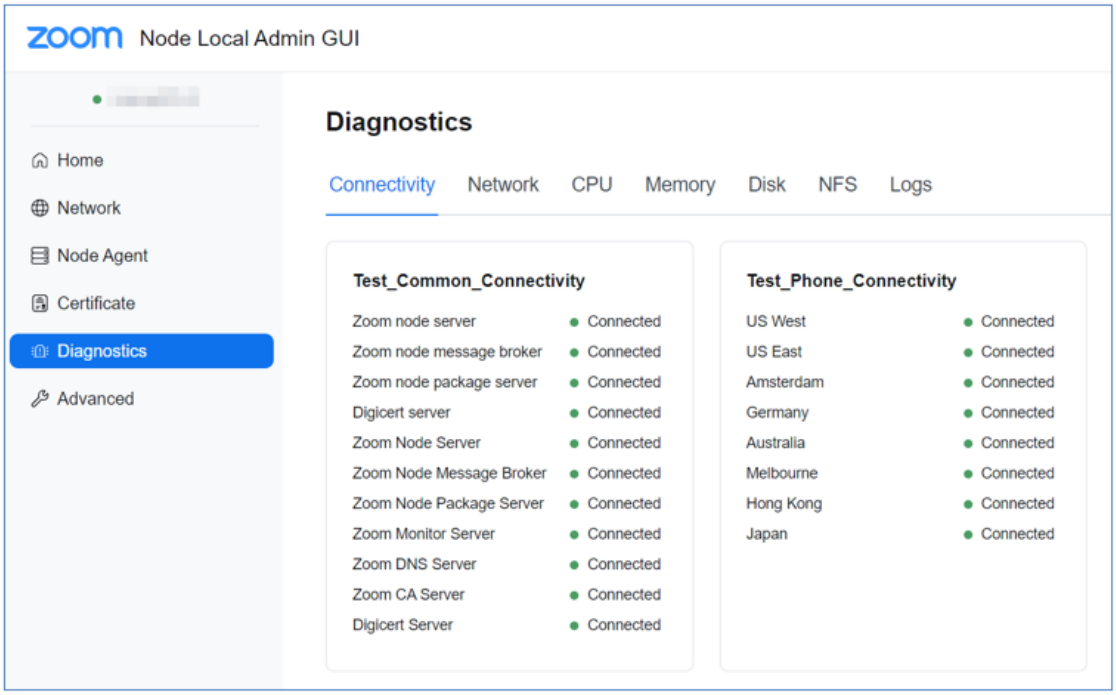
2. Log in with the password of the "zoom-setup" user that you configured during the initial setup.



3. From the left navigation menu, click **Diagnostics**.



4. Under the **Connectivity** tab, verify all connections are listed as "Connected":



5. If any of the connection tests fail, please review the Zoom Node firewall documentation and ensure your firewall allows communication to the destination addresses via the required ports.

Zoom Node Registration

Once connectivity to the Zoom Cloud has been established and verified, the Zoom Node is ready to be registered within the Zoom web portal. The first step is to generate code through

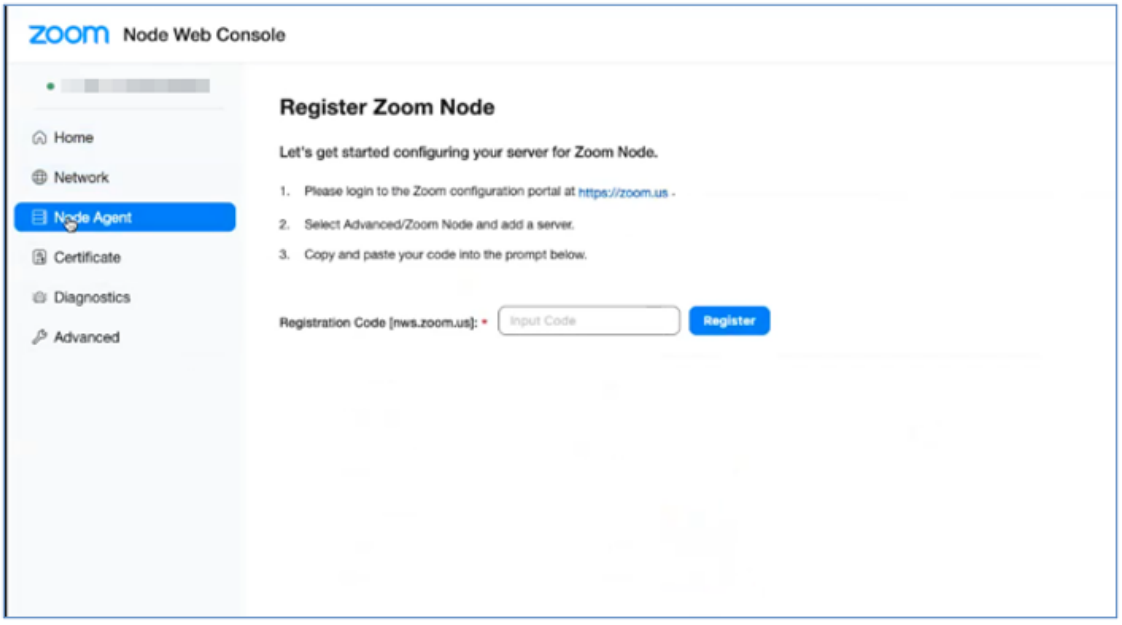
Zoom web portal.

➢ To generate registration code:

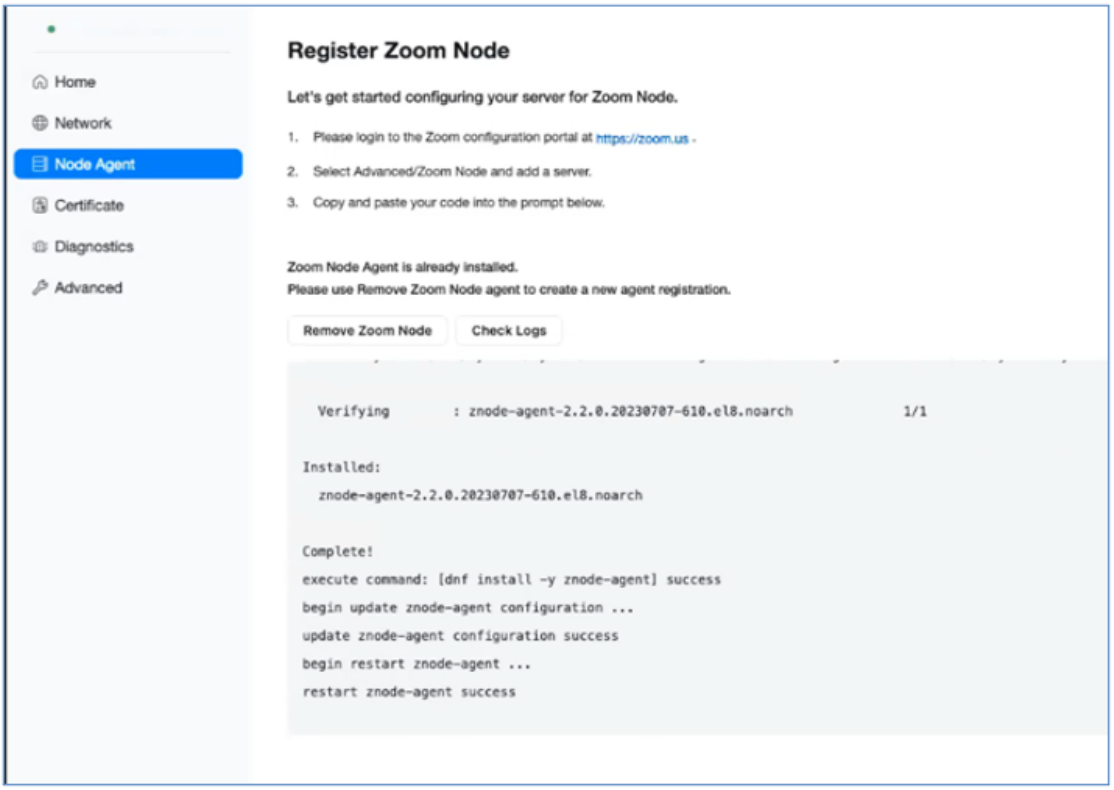
1. Sign-in to the Zoom web portal at https://zoom.us.
2. In the navigation menu, click **Node Management**, and then click **Modules**.
3. Click **Nodes**.
4. Click **Add Nodes**; a dialog box appears.
5. (Optional) Set the time for the Code Expiration in minutes.
6. Click **Generate**.
7. Click **Copy** to copy the registration code and save it for use later.

➢ To register Zoom Node:

1. Navigate back to the Zoom Node web console at **https://[IPaddress]:8443**, and then click **Node Agent**.
2. Enter the registration code that you copied from the Zoom admin portal in the previous step, and then click **Register**.



3. Once the agents have installed and registered, a message appears that the installation was successful.



4. Return to the Zoom web portal, and under the **Nodes** tab, click **Unconfirmed Nodes**; the newly added server is now listed under **Unconfirmed Nodes**.
5. Click **Confirm** to authorize and complete the server registration.
6. In the next window enter the following information:
   - **Description:** Description of the server.
   - **Location:** Location of the server, which should be listed in a way to easily filter in the **Servers** tab.
7. Click **Confirm**.
8. Click the **Confirmed Nodes** tab to view the registered server.
9. Click the name of the server to view the server's properties.
10. Navigate to the **Agents** tab to ensure that the **Node Agent** and **Monitor Agent** are running before proceeding. It may take a few minutes for both, to become available.
11. The Zoom Node server is now ready to deploy services and modules.

Zoom Phone Local Survivability Module Setup

This section describes how to configure the ZPLS module before starting the service for use in a failover situation.

Information in this section is based on official Zoom Support documentation, which may be updated from time to time by Zoom.

Adding Local Survivability Service

Once the Zoom Node virtual machine has been deployed and registered, you can deploy the Local Survivability module on the server.

➢ **To add Local Survivability service:**

1. Sign-in to the Zoom web portal at https://zoom.us.
2. In the navigation menu, click **Node Management**, and then click **Modules**.
3. Under the **Services** tab, click **Add Services**; a dialog box appears.
4. Click **Local Survivability**.
5. Fill in the following information:
   - **Install on a Node:** Select the Zoom Node Phone server where the module will be deployed.
   - **Internal IP:** Configure the internal IP address used for the module (based on the example above, 10.15.77.51)
6. Optionally, you can add an internal domain.
7. Click **Add**; installation on the server of the Local Survivability module and components begins. Once complete, the status of the module changes to "Stopped".

DO NOT start the module until it has been assigned to a site.

Assigning Local Survivability Server to Site

After the ZPLS module has been setup, you need to assign it to a site.

➢ **Assign a Local Survivability Server to a site:**

1. Sign-in to the Zoom web portal at https://zoom.us.
2. In the Navigation menu, click **Phone System Management**, and then click **Company Info**.
3. Click **Account Settings**.
4. Under **Zoom Node**, locate **Local Survivability**.
5. Click **Manage**.
6. Click **Assign to**.
7. Select the site the server will be assigned to, and then click **OK**.
8. Click **Save**.

9. In the navigation menu, click **Node Management**, and then click **Modules**.
10. Click the **Services** tab and then click **Start**.

Integrating SBC with ZPLS Module

This section describes the steps required for assigning the SBC to the ZPLS module. If Inbound and Outbound PSTN connectivity in failover mode is required, customers will be required to set up Trunk Groups and SBCs within the Zoom Admin portal.

Adding the SBC within the Administration portal does not directly create the SIP Trunk between the ZPLS module and SBC. The SBC needs to be associated with a Survivability Route Group which is then associated with the appropriate Site/Account - only at this stage is the ZPLS module made aware of the IP Address details of the SBC that is used for external call routing.

➢ **To integrate SBC with ZPLS module:**

1. Sign-in to the Zoom web portal at https://zoom.us.
2. In the Navigation menu, click **Phone System Management**, and then click **Company Info**.
3. Click **Account Settings**.
4. Under **Routing**, locate **Session Border Controllers**.
5. Click **Manage**.
6. Click **Add**.
7. Enter the **Display name** and **Public IP address** for the SBC. The IP address for the SBC needs to be reachable from the ZPLS module over port 5061. If utilizing 1:1 NAT, the addresses must be static.
8. Enable **Bring Your Own PBX - Premises** to ensure that BYOC numbers are routed correctly under normal conditions.
9. Enable **OPTIONS Ping Status**, which allows admins to verify the SIP Trunk connections between the SBC as well as the ZPLS module and the Zoom Phone Cloud.
10. Enable **In Service**.
11. For **Survivability Public/Private IP Address** enter the private (LAN) IP address of the SBC. This address is utilized by the module once the **Survivability Route Group** has been added to a site. This is an optional setting that must be configured if the SBC is being leveraged by the ZPLS module. This is usually a private IP address of the SBC that is synchronized with the ZPLS module and is used for PSTN call routing in the event of an outage at the specific site.

Zoom recommends utilizing the private address to avoid routing through the firewall and potentially needing to add complete route reflection rules.

12. Click **Save**.

Assigning SBC to a Route Group

Two **Route Groups** should be created at the Account or Phone Site to ensure PSTN connectivity is functional with the survivability solution:

- A Route Group is needed for assignment to the specific Phone System Site that is enabled for survivability - the Survivability Public/Private IP Address defined within the SBC is pushed to the ZPLS module. Upon entering failover mode, ZPLS sends external calls to the SBC IP Address contained within the Survivability Route Group. This Route Group does not contain a "Region" since the purpose of this Route Group is to establish a connection to the ZPLS module.
- At least one additional Route Group is required for routing incoming calls to BYOC numbers during normal conditions. In this instance, a SIP Trunk is created between the Zoom Phone SIP Zone(s) contained within the Region(s) and the SBC Public IP Address. Backup **Route Groups** are possible with this BYOC Route Group but not the survivability Route Group.

➢ To add Route Group for Local Survivability:

1. Sign-in to the Zoom web portal at https://zoom.us.
2. In the Navigation menu, click **Phone System Management**, and then click **Company Info**.
3. Click **Account Settings**, locate **Route Groups**, and then click **Manage**.
4. Click **Add**.
5. Enter a Display Name for the Route Group.
6. Change the Type to **Survivability**.
7. Select the **Session Border Controller** added in the previous step.
8. Click **Save**.

➢ To add another Route Group for BYOC:

1. On the same page (**Route Groups**), click **Add**.
2. Enter a Display Name for the Route Group.
3. Change the Type to **BYOC-P**.
4. From the Region drop menu, select the appropriated region.
5. Select the Session Border Controller added in the previous step.
6. Click **Save**.
7. Click **Provision** for the created BYOC Route Group.

➢ To assign a Route group to a ZPLS module:

1. In the Navigation menu, click **Phone System Management**, and then click **Company Info**.
2. Click **Account Settings**.

3. Under **Zoom Node**, locate **Local Survivability**.
4. Click **Manage**.
5. Click **Edit**, and in the Assign to, select the survivability Route Group (created in the previous step). The selected Server should be assigned to a specific Site and when PSTN connectivity is required the survivability Route Group should also be assigned.
6. Select the **Route Group** created in the previous step.
7. Click **OK**.

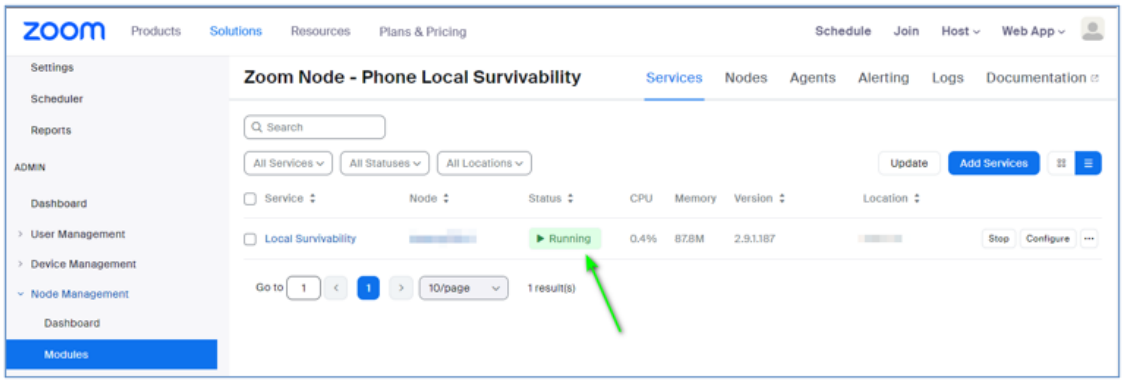
Testing the ZPLS Service Module

This section describes the steps for testing proper configuration of the ZPLS module. For this purpose, zoom administrators can simulate a failover to verify the service is working as intended.

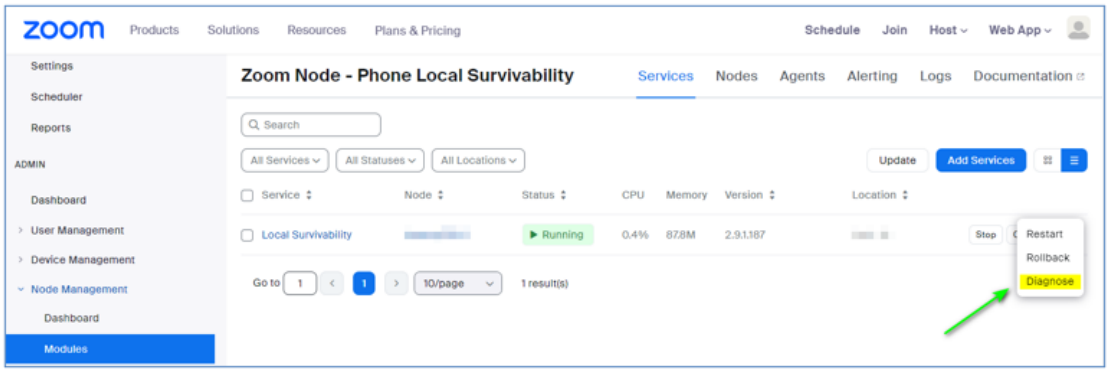
> Network connectivity to Zoom Cloud from the Zoom Node server can be verified via the Virtual Machine itself. See Test Zoom Node Network Connectivity on page 16.

➢ **To test and validate Local Survivability configuration:**

1. In the navigation menu, click **Node Management**, and then click **Modules**.
2. Click the **Services** tab.
3. Locate the **Local Survivability** service.
4. Verify the status is Running and there is not any fault information:



5. Click the dots at the end of the line and select **Diagnose** to run diagnostic tests for all services.



6. Check that diagnostic tests for all services are "OK". If they are not "OK", find the reason and act according to the procedure in the solution.

Simulating a Failover

To test the Local Survivability service module, an internet outage needs to be simulated by disconnecting your internet connection or by creating firewall rules to block access to the Zoom Phone networks. To determine the Zoom Phone network, please reference the Zoom Support article for Network Firewall or Proxy Server Settings and refer to the Zoom Phone section for the IP addresses and port numbers you should block.

The Zoom desktop client and physical phones should detect network loss and connect to the Local Survivability node. The Zoom desktop clients will show a loss of connection.

➢ **To validate that the Zoom soft clients are registered to the Local Survivability service module:**

On the Zoom client:

1. Click the Profile picture or icon in the upper right.
2. Select **Settings**.
3. Click **Statistics**.
4. Click **Phone**.
5. Verify the Register Server IP/Port is that of your Zoom Node.

Testing Mode

Admins can bypass creating firewall rules to simulate failover by enabling Testing Mode. Testing Mode removes the need to block cloud connectivity from the desktop client and ZPLS module.

➢ **To enable Testing Mode:**

1. Sign-in to the Zoom web portal at https://zoom.us.
2. In the Navigation menu, click **Phone System Management**, and then click **Company Info**.
3. Click **Account Settings**.

4. Under Zoom Node, locate **Local Survivability**.
5. Click **Manage**.
6. Click **Local Survivability**, and then click **Edit**.
7. Enable **Testing Mode**.
8. Restart the ZPLS module.

New registrations from clients within the associated Site register to the ZPLS module as opposed to the cloud. Testing Mode is only active once the ZPLS module has been restarted. Users should log out and log back into the client to verify Local Survivability. Testing Mode is restricted to the Desktop client and does not affect physical devices.

7 Configuring AudioCodes Mediant 800C SBC

This section describes how to configure AudioCodes SBC for interworking between the ZPLS, the Zoom Phone Cloud system and the Generic SIP Trunk. These configuration procedures are based on the typical deployment topology described in Deployment Topology on page 3, and includes the following main areas:

- SBC LAN interface: ZPLS module and Management Station.
- SBC WAN interface: Generic SIP Trunking and the Zoom Phone Cloud system environment.

This configuration is done using the SBC's embedded Web server (hereafter, referred to as Web interface).

Validating AudioCodes SBC License and Version

Zoom has successfully conducted validation tests with AudioCodes' Mediant SBC Ver. 7.40A.250. The previous certified firmware version is 7.20A.258.

- For interconnection between the ZPLS module, the Zoom Phone Cloud system, and Generic SIP Trunk based on the configuration described in this section, AudioCodes SBC must be installed with a License Key that includes the following software features:
  - ✓ Number of SBC sessions [Based on requirements]
  - ✓ DSP Channels [If media transcoding is needed]
  - ✓ Transcoding sessions [If media transcoding is needed]
  - ✓ Coders [Based on requirements]

  For more information about the License Key, contact your AudioCodes sales representative.
- If your SBC is deployed in a virtual environment and transcoding is required, your virtual machine must have a minimum of two vCPUs. For more information, please refer to the appropriate Installation Manual, which can be found on AudioCodes website.
- The scope of this document does not cover all security aspects for configuring this topology. Comprehensive security measures should be implemented per your organization's security policies. For security recommendations on AudioCodes' products, refer to the Recommended Security Guidelines document, which can be found at AudioCodes website.

Prerequisites

Before you begin configuration, make sure you have obtained the following for each SBC you wish to pair with Zoom Phone Systems:

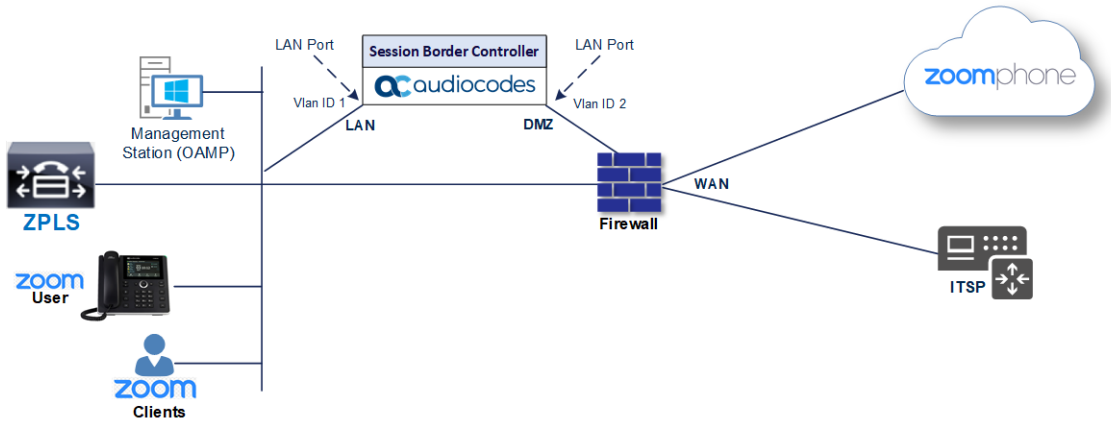
- Public IP address
- Public certificate that is issued by one of the Zoom supported CAs

Configuring IP Network Interfaces

This section describes how to configure the SBC's IP network interfaces. There are several ways to deploy the SBC; however, deployment topology, explained in this document employs the following method:

- SBC interfaces with the following IP entities:
  - ZPLS module and Management Servers located on the LAN.
  - Zoom Phone Cloud System and Generic SIP Trunk, located on the WAN.
- SBC connects to the WAN through a DMZ network.
- Physical connection: The type of physical connection depends on the method used to connect to the Enterprise's network. In the typical deployment topology, SBC connects to the LAN and DMZ using dedicated Ethernet ports (i.e., two ports and two network cables are used).
- SBC also uses two logical network interfaces:
  - LAN (VLAN ID 1)
  - DMZ (VLAN ID 2)

Figure 7-1: Network Interfaces in Typical Deployment Topology



Configuring LAN and WAN VLANs

This section describes how to configure VLANs for each of the following interfaces:

- LAN (assigned the name "LAN_IF")
- WAN (assigned the name "WAN_IF")

➢ **To configure the VLANs:**

1. Open the Ethernet Device table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **Ethernet Devices**).

   There is one existing row for VLAN ID 1 and underlying interface GROUP_1.

2. Add another VLAN ID 2 for the WAN side.

Configuring Network Interfaces

This section describes how to configure the IP network interfaces for each of the following interfaces:

- LAN Interface (assigned the name "LAN_IF")
- WAN Interface (assigned the name "WAN_IF")

➢ **To configure the IP network interfaces:**

1. Open the IP Interfaces table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **IP Interfaces**).
2. Configure the IP interfaces as follows (your network parameters might be different):

Table 7-1: Configuration Example of the Network Interface Table

Index	Application Types	Interface Mode	IP Address	Prefix Length	Gateway	DNS	I/F Name	Ethernet Device
0	OAMP+ Media + Control	IPv4 Manual	10.15.77.60	16	10.15.0.1	10.15.27.1	LAN_IF	vlan 1
1	Media + Control (as this interface points to the Internet, enabling OAMP is not recommended)	IPv4 Manual	195.189.192.153 (DMZ IP address of SBC)	25	195.189.192.129 (router's IP address)	According to your Internet provider's instructions	WAN_IF	vlan 2

Configuring TLS Context for Zoom

This section describes how to configure the SBC for using a TLS connection with the Zoom Phone Cloud System. This configuration is essential for a secure SIP TLS connection.

The procedure involves the following main steps:

- Configuring NTP Server Address on the next page
- Creating a TLS Context for Zoom Phone System on the next page

- Generating a CSR and Obtaining Certificate from Supported CA below
- Deploying SBC Signed and Trusted by Zoom Root Certificates on the next page

Configuring NTP Server Address

This section describes how to configure the NTP server's IP address. it's recommended to implement an NTP server (local NTP server or another global NTP server) to ensure that the SBC receives the current date and time. This is necessary for validating certificates of remote parties. It's important that the NTP server be located on the OAMP IP Interface (LAN_IF in our case) or be accessible through it.

➢ **To configure NTP server address:**

1. Open the Time & Date page (**Setup** menu > **Administration** tab > **Time & Date**).
2. In the 'Primary NTP Server Address' field, enter the IP address of the NTP server (e.g., 10.15.27.1).
3. Click **Apply**.

Creating a TLS Context for Zoom Phone System

The section below describes how to request a certificate for the SBC WAN interface and configure it. The certificate is used by the SBC to authenticate the connection with the Zoom Phone System.

➢ **To create a TLS Context for Zoom Phone System:**

1. Open the TLS Contexts page (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
2. Create a new TLS Context by clicking +**New**, and then configure the parameters using the following table as reference.

Table 7-2: New TLS Context

Index	Name	TLS Version
1	Zoom (arbitrary descriptive name)	TLSv1.2 and TLSv1.3
All other parameters can be left unchanged with their default values.		

3. Click **Apply**; you should see the new TLS Context and option to manage the certificates at the bottom of 'TLS Context' table.

Generating a CSR and Obtaining Certificate from Supported CA

This section describes how to generate a Certificate Signing Request (CSR) and obtain the certificate from a supported Certification Authority (CA).

> Currently, Zoom doesn't officially support the use of wildcard certificates. However, Zoom doesn't validate the CN or SAN.

➢ **To generate CSR and obtain certificate from supported CA:**

1. Open the TLS Contexts page (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
2. In the TLS Contexts page, select the Zoom TLS Context index row, and then click the **Change Certificate** link located below the table; the Context Certificates page appears.
3. Under the Certificate Signing Request group, do the following:
   a. In the 'Common Name [CN]' field, enter the SBC FQDN name (e.g., zpls-sbc.audiocodes.com).
   b. In the '1st Subject Alternative Name [SAN]' field, change the type to **DNS** and enter the SBC FQDN name (based on example above, zpls-sbc.audiocodes.com).
   c. Fill in the rest of the request fields according to your security provider's instructions.
   d. Click the **Create CSR** button; a textual certificate signing request is displayed in the area below the button.
4. Copy the CSR from the line "----BEGIN CERTIFICATE REQUEST" to "END CERTIFICATE REQUEST----" to a text file (such as Notepad), and then save it to a folder on your computer with the file name, for example certreq.txt.
5. Send certreq.txt file to the Certified Authority Administrator for signing.

Deploying SBC Signed and Trusted by Zoom Root Certificates

After obtaining the SBC signed certificate from the CA, download trusted by Zoom Public Root Certificates and install the following:

- SBC certificate signed by the public CA authority that was authorized by Zoom (see Zoom Public Trusted Certificate List on page 57).
- Trusted by Zoom Public Root certificates.

Currently, Zoom Data Centers (DC) uses DigiCert public CA certificates. Zoom is in the process of transitioning the root certificate to **DigiCert Global Root G2** and **DigiCert TLS RSA4096 Root G5**, which begins after December 1, 2023. Therefore, to establish a TLS connection with Zoom Phone infrastructure, download and install as a trusted root the following public CA certificates:

- https://cacerts.digicert.com/DigiCertGlobalRootG2.crt.pem
- https://cacerts.digicert.com/DigiCertTLSRSA4096RootG5.crt.pem
- https://cacerts.digicert.com/DigiCertGlobalG2TLSRSASHA2562020CA1-1.crt.pem
- https://cacerts.digicert.com/DigiCertG5TLSRSA4096SHA3842021CA1-1.crt.pem

➢ **To install the SBC certificate:**

1. In the SBC's Web interface, return to the TLS Contexts page and do the following:
   a. In the TLS Contexts page, select the required TLS Context index row, and then click the **Change Certificate** link located below the table; the Context Certificates page appears.
   b. Scroll down to the Upload certificates files from your computer group, click the **Choose File** button corresponding to the 'Send Device Certificate...' field, navigate to the certificate file obtained from the CA, and click **Load File** to upload the certificate to the SBC.
2. Validate that the certificate was uploaded correctly. A message indicating that the certificate was uploaded successfully is displayed in blue in the lower part of the page.
3. In the SBC's Web interface, return to the TLS Contexts page, select the required TLS Context index row, and then click the **Certificate Information** link, located at the bottom of the TLS. Then validate the Key size, certificate status and Subject Name.
4. In the SBC's Web interface, return to the TLS Contexts page.
   a. In the TLS Contexts page, select the required TLS Context index row, and then click the **Trusted Root Certificates** link, located at the bottom of the TLS Contexts page; the Trusted Certificates page appears.
   b. Click the **Import** button, and then select all trusted by Zoom public CA certificates (obtained from the link at the beginning of this section) to load.
5. Click **OK**; the certificate is loaded to the device and listed in the Trusted Certificates store.

The above method creates a signed certificate for an explicit device, on which a Certificate Sign Request was generated (and signed with private key).

Configuring Media Realms

This section describes how to configure Media Realms. Media Realms allows the dividing of the UDP port ranges for use on different interfaces. In the example below, the following Media Realms are configured:

- One for the IP interface towards the ZPLS module, with the UDP port starting at 20000 and the number of media session legs is 100 (you need to calculate number of media session legs based on your usage).
- One for the IP interface towards the Zoom Phone Cloud System, with the UDP port starting at 10000 and the number of media session legs 100 (you need to calculate number of media session legs based on your usage).
- One for the IP interface towards Generic SIP Trunk, with the UDP port range starting at 6000 and the number of media session legs 100.

➢ **To configure Media Realms:**

1. Open the Media Realms table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Media Realms**).
2. Configure Media Realm as follows:

If you use the default Media Realm (Index 0), you must modify it.

Table 7-3: Configuration Example Media Realms in Media Realm Table

Index	Name	IPv4 Interface Name	Port Range Start	Number of Media Session Legs
0	MR-ZPLS (arbitrary name)	LAN_IF	20000	100 (media sessions assigned with port range)
1	MR-Zoom (arbitrary name)	WAN_IF	10000	100 (media sessions assigned with port range)
2	MR-SIPTrunk (arbitrary name)	WAN_IF	6000	100 (media sessions assigned with port range)
All other parameters can be left unchanged at their default values.				

Configuring SIP Signaling Interfaces

This section describes how to configure a SIP Signaling Interfaces. A SIP Interface defines a listening port and type (UDP, TCP, or TLS) for SIP signaling traffic on a specific logical IP network interface (configured in the Interface Table above) and Media Realm.

Note that the configuration of a SIP Interface for the Generic SIP Trunk shows an example, and your configuration might be different. For specific configuration of interfaces pointing to SIP trunks and/or a third-party PSTN environment connected to the SBC, see the trunk / environment vendor documentation.

AudioCodes also offers a comprehensive suite of documents covering the interconnection between different trunks and equipment.

➢ **To configure SIP Interfaces:**

1. Open the SIP Interfaces table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **SIP Interfaces**).
2. Configure SIP Interfaces. You can use the default SIP Interface (Index 0), but modify it as shown in the following table. The following table shows an example of the configuration. You can change some parameters according to your requirements.

Table 7-4: Configured SIP Interfaces in SIP Interface Table

Index	Name	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	Media Realm
0	SI_ZPLS (arbitrary name)	LAN_IF	**SBC**	0	0	5061 (according to requirement)	MR-ZPLS
1	SI_Zoom (arbitrary name)	WAN_IF	**SBC**	0	0	5061 (according to requirement)	MR-Zoom
2	SI_ SIPTrunk (arbitrary name)	WAN_IF	**SBC**	5060 (according to requirement)	0	0	MR-SIP Trunk
All other parameters can be left unchanged at their default values.							

For enhanced security, AudioCodes recommends implementing a Mutual TLS connection with the Zoom Phone System. For required configuration, see Configuring Mutual TLS Authentication for SIP on page 54.

Configuring Proxy Sets and Proxy Address

This section describes how to configure Proxy Sets. The Proxy Set defines the destination address (IP address or FQDN) of the IP entity server. Proxy Sets can also be used to configure load balancing between multiple servers.

For the typical deployment topology, Proxy Sets need to be configured for the following IP entities:

- ZPLS module
- Zoom Phone Cloud System
- Generic SIP Trunk

The Proxy Sets will later be applied to the VoIP network by assigning them to IP Groups.

➢ **To configure Proxy Sets:**

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**).
2. Configure Proxy Sets as shown in the following table:

Table 7-5: Configuration Example Proxy Sets in Proxy Sets Table

Index	Name	SBC IPv4 SIP Interface	TLS Context Name	Proxy Keep-Alive	Keep-Alive Failure Responses	Redundancy Mode	Proxy Hot Swap
1	ZPLS (arbitrary name)	SI_ZPLS	Zoom (configured in Configuring TLS Context for Zoom on page 28)	**Using Options**	-	-	-
2	Zoom DCs (arbitrary name)	SI_ Zoom	Zoom (configured in Configuring TLS Context for Zoom on page 28)	**Using Options**	**503**	**Homing**	**Enable**
3	SIPTrunk (arbitrary name)	SI_ SIPTrunk	Default	**Using Options**	According to SIP Trunk requirement	According to SIP Trunk requirement	According to SIP Trunk requirement

On Hybrid SBCs (with onboard PSTN interfaces) it's recommended to leave Proxy Set 0 unconfigured for possible future use for PSTN Fallback.

Configuring a Proxy Address

This section describes how to configure a Proxy Address.

➢ **To configure a Proxy Address for ZPLS module:**

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**).
2. Click the Proxy Set ZPLS, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.
3. Click +**New**, and then configure the address of the Proxy Set according to the parameters described in the following table:

Table 7-6: Configuration Proxy Address for ZPLS Module

Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	10.15.77.51:5061 (ZPLS module IP and port in our example)	TLS	0	0

4. Click **Apply**.

➢ **To configure a Proxy Address for Zoom:**

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**).
2. Click the Proxy Set Zoom Cloud, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.
3. Click +**New**, and then configure the address of the Proxy Set according to the parameters described in the following table:

Table 7-7: Configuration Proxy Address for Zoom Phone Cloud System

Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	213.19.144.198:5061	TLS	0	0
1	213.19.140.198:5061	TLS	0	0

4. Click **Apply**.

The current example is based on configuration Zoom Europe Data Center's IP address. In your implementation, the IP address may be different according to your region. See Zoom Data Centers on page 55 for a list of FQDNs / IP addresses of other Zoom Regional Data Centers. Zoom prefer to use IP addresses instead of FQDNs.

➢ **To configure a Proxy Address for SIP Trunk:**

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**)
2. Click the Proxy Set SIPTrunk, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.
3. Click +**New**, and then configure the address of the Proxy Set according to the parameters described in the following table:

Table 7-8: Configuration Proxy Address for SIP Trunk

Index	Proxy Address	Transport Type	Proxy Priority	Proxy Random Weight
0	SIPTrunk.com:5060 (SIP Trunk IP / FQDN and port)	UDP	0	0

4. Click **Apply**.

Configuring Coders

This section describes how to configure coders (termed Coder Group). The Zoom Phone system supports the OPUS and G.722 coders while the network connection to Generic SIP Trunk may restrict operation with other dedicated coders list. Therefore, you may need to add a Coder Group with the supported coders for each leg, the Zoom Phone systems, and the Generic SIP Trunk.

The Coder Group ID for this entity is assigned to its corresponding IP Profile in the next step.

➢ **To configure coders for Zoom Phone systems:**

1. Open the Coder Groups table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > Coder Groups).
2. From the 'Coder Group Name' drop-down, select **1:Does Not Exist** and add the required coders as follows:

Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression
Opus	20	N/A	102	N/A
G.722	20	64	9	Disabled

3. Click **Apply** and confirm the configuration change in the prompt that pops up.

Repeat the same procedure for each Generic SIP Trunk if required.

The procedure below describes how to configure Allowed Coders Groups to ensure that voice sent to the Generic SIP Trunk and Zoom Phone systems, uses the dedicated coders list whenever possible. Note that the Allowed Coders Group IDs are assigned to the IP Profiles belonging to the Generic SIP Trunk and Zoom Phone systems, in the next step.

➢ **To set a preferred coder for the Generic SIP Trunk:**

1. Open the Allowed Audio Coders Groups table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **Allowed Audio Coders Groups**).
2. Click **New**, and then configure a name for the Allowed Audio Coders Group for Generic SIP Trunk (e.g., SIPTrunk Allowed Coders).
3. Click **Apply**.
4. Select the new row that you configured, and then click the **Allowed Audio Coders** link located below the table; the Allowed Audio Coders table opens.
5. Click **New** and configure an Allowed Coders as follows:

Index	Coder
0	G.729
1	G.711 U-law
2	G.711 A-law

➢ **To set a preferred coder for the Zoom Phone systems:**

1. Open the Allowed Audio Coders Groups table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **Allowed Audio Coders Groups**).
2. Click **New**, and then configure a name for the Allowed Audio Coders Group for Zoom Phone system (e.g., Zoom Allowed Coders).
3. Click **Apply**.
4. Select the new row that you configured, and then click the **Allowed Audio Coders** link located below the table; the Allowed Audio Coders table opens.
5. Click **New** and configure an Allowed Coders as follows:

Index	Coder
0	Opus
1	G.711 U-law

Index	Coder
2	G.711 A-law
3	G.722

6. Open the Media Settings page (**Setup** menu > **Signaling & Media** tab > **Media** folder > **Media Settings**).
7. From the 'Extended Coders Behavior' drop-down list, select **Include Extensions**.
8. Click **Apply**.

Configuring IP Profiles

This section describes how to configure IP Profiles. The IP Profile defines a set of call capabilities relating to signaling (e.g., SIP message terminations such as REFER) and media (e.g., coder and transcoding method).

➢ **To configure IP Profile for the Zoom Phone system:**

1. Open the IP Profiles table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **IP Profiles**).
2. Click +**New** and add the IP Profile for Zoom Phone System interface. Configure the parameters using the following table as reference.

Table 7-9: Configuration Example: Zoom IP Profile

Parameter	Value
General	
Index	1
Name	Zoom (arbitrary descriptive name)
Media Security	
SBC Media Security Mode	**Secured**
SBC Media	
Extension Coders Group	**AudioCodersGroups_1**
Allowed Audio Coders	**Zoom Allowed Coders**

Parameter	Value
Allowed Coders Mode	**Restriction and Preference** (reorder coders according to allowed Coders including extension coders)
RFC 2833 Mode	**Extend**
SBC Signaling	
Session Expires Mode	**Supported**
All other parameters can be left unchanged with their default values.	

3. Click **Apply**.

➢ **To configure an IP Profile for the Generic SIP Trunk:**

1. Open the IP Profiles table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **IP Profiles**).
2. Click +**New** add the IP Profile for the Generic SIP Trunk. Configure the parameters using the following table as reference.

Table 7-10: Configuration Example: Generic SIP Trunk IP Profile

Parameter	Value
General	
Index	2
Name	SIPTrunk
Media Security	
SBC Media Security Mode	**Not Secured**
SBC Media	
Extension Coders Group	**AudioCodersGroups_2**
Allowed Audio Coders	**SIPTrunk Allowed Coders**
Allowed Coders Mode	**Restriction and Preference** (reorder coders according to Allowed Coders including extension coders)

Parameter	Value
SBC Signaling	
P-Asserted-Identity Header Mode	**Add** (required for anonymous calls)

3. Click **Apply**.

Configuring SIP Response Codes for Alternative Routing Reasons

This section describes how to configure the SBC's handling of SIP error responses received from Zoom Phone Cloud system for outgoing SIP dialog-initiating methods (e.g., INVITE, OPTIONS, and SUBSCRIBE messages). In this case, the SBC attempts to locate an alternative route for the call. This feature works together with the Proxy Hot Swap feature, which is configured in the Proxy Sets table. Alternative routing based on SIP responses is configured using two tables with 'parent-child' relationships:

- Alternative Reasons Set table ('parent'): Defines the name of the Alternative Reasons Set.
- Alternative Reasons Rules table ('child'): Defines SIP response codes per Alternative Reasons Set.

To **Apply** your configured alternative routing reason rules, you need to assign the Alternative Reasons Set for which you configured the rules, to the Zoom Phone Cloud system IP Group in the IP Groups table, using the 'SBC Alternative Routing Reasons Set' parameter.

➢ **To configure SIP reason codes for alternative IP routing:**

1. Open the Alternative Routing Reasons table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **Alternative Reasons Set**).
2. Click **New** and configure a name for the Alternative Routing Reasons Set (e.g., Alt. Route Reasons).
3. Click **Apply**.
4. Select the index row of the Alternative Reasons Set that you added, and then click the **Alternative Reasons Rules** link located at the bottom of the page; the Alternative Reasons Rules table opens.
5. Click **New** and select **503 Service Unavailable** from the 'Release Cause Code' drop-down list.
6. Click **Apply**.

Additional SIP responses can be added to the table, based on requirements.

Configuring IP Groups

This section describes how to configure IP Groups. The IP Group represents an IP entity on the network with which the SBC communicates. This can be a server (e.g., IP PBX or ITSP) or it can be a group of users (e.g., LAN IP phones). For servers, the IP Group is typically used to define the server's IP address by associating it with a Proxy Set. Once IP Groups are configured, they are used to configure IP-to-IP routing rules for denoting source and destination of the call.

In this typical deployment topology, IP Groups must be configured for the following IP entities:

- ZPLS module
- Zoom Phone Cloud System
- Generic SIP Trunk

➢ **To configure IP Groups:**

1. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
2. Configure an IP Group for the ZPLS module:

Parameter	Value
Index	1
Name	ZPLS (arbitrary descriptive name)
Type	**Server**
Proxy Set	**ZPLS**
IP Profile	**Zoom**
Media Realm	**MR- ZPLS**
SIP Group Name	(According to requirement)
Proxy Keep-Alive using IP Group settings	**Enable**
All other parameters can be left unchanged with their default values.	

3. Configure an IP Group for the Zoom Phone Cloud system:

Parameter	Value
Index	2

Parameter	Value
Name	Zoom Cloud (arbitrary descriptive name)
Type	**Server**
Proxy Set	**Zoom Cloud**
IP Profile	**Zoom**
Media Realm	**MR-Zoom**
SIP Group Name	(According to requirement)
SBC Alternative Routing Reason Set	**Alt. Route Reasons** (created in Configuring SIP Response Codes for Alternative Routing Reasons on page 40)
Proxy Keep-Alive using IP Group settings	**Enable**
All other parameters can be left unchanged with their default values.	

4. Configure an IP Group for the SIP Trunk:

Parameter	Value
Index	3
Name	SIPTrunk (arbitrary descriptive name)
Type	**Server**
Proxy Set	**SIPTrunk**
IP Profile	**SIPTrunk**
Media Realm	**MR-SIPTrunk**
SIP Group Name	(According to ITSP requirement)
All other parameters can be left unchanged with their default values.	

On Hybrid SBCs (with onboard PSTN interfaces) it's recommended to leave IP Group 0 unconfigured for possible future use for PSTN Fallback.

Configuring SRTP

This section describes how to configure media security. This section describes how to configure media security. The Zoom Phone System Interface needs to use SRTP only, so you need to configure the SBC to operate in the same manner. By default, SRTP is disabled.

➢ **To configure media security:**

1. Open the Media Security page (**Setup** menu > **Signaling & Media** tab > **Media** folder > **Media Security**).
2. From the 'Media Security' drop-down list, select **Enable** to enable SRTP.
3. Click **Apply**.

Configuring IP-to-IP Call Routing Rules

This section describes how to configure IP-to-IP call routing rules. These rules define the routes for forwarding SIP messages (e.g., INVITE) received from one IP entity to another. The SBC selects the appropriate rule based on matching characteristics (e.g., IP Group) of the incoming SIP message. If the input characteristics do not match the first rule in the table, they are compared to the next rule, and so on, until a matching rule is located. If no rule is matched, the message is rejected.

In a typical deployment topology, the following IP-to-IP routing rules must be configured:

- Terminate SIP OPTIONS messages on the SBC that are received from any entity.
- Calls from Zoom Phone Cloud system to Generic SIP Trunk.
- Calls from Generic SIP Trunk to Zoom Phone Cloud system.
- If the Zoom Phone Cloud system is not available, route calls from the Generic SIP Trunk to the ZPLS module.
- Calls from ZPLS module to Generic SIP Trunk.

➢ **To configure IP-to-IP routing rules:**

1. Open the IP-to-IP Routing table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **IP-to-IP Routing**).
2. Configure routing rules as shown in the following table:

Table 7-11: Configuration IP-to-IP Routing Rules

Index	Name	Alternative Route Options	Source IP Group	Request Type	Dest Type	Dest IP Group	Internal Action
0	Terminate		**Any**	**OPTIONS**	**Internal**		**Reply** (Response='2

Index	Name	Alternative Route Options	Source IP Group	Request Type	Dest Type	Dest IP Group	Internal Action
	OPTIONS						00')
1	Zoom to ITSP (arbitrary name)		**Zoom Cloud**		**IP Group**	**SIPTrunk**	
2	ITSP to Zoom (arbitrary name)		**SIPTrunk**		**IP Group**	**Zoom Cloud**	
3	ITSP to ZPLS (arbitrary name)	**Alternative Route Ignore Inputs**	**SIPTrunk**		**IP Group**	**ZPLS**	
4	ZPLS to ITSP (arbitrary name)		**ZPLS**		**IP Group**	**SIPTrunk**	

The routing configuration may change according to your specific deployment topology.

Configure Number Manipulation Rules

This section describes how to configure IP-to-IP manipulation rules. These rules manipulate the SIP Request-URI user part (source or destination number). The manipulation rules use the configured IP Groups (as configured in Configuring IP Groups on page 41) to denote the source and destination of the call.

Adapt the manipulation table according to your environment dial plan.

In this specific deployment topology, a manipulation is configured to add the "+" (plus sign) to the destination number (if it's not already present) for calls from the Generic SIP Trunk IP Group to the Zoom Phone Cloud System IP Group, regardless of any destination username pattern.

➢ **To configure a number manipulation rule:**

1. Open the Outbound Manipulations table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Manipulation** > **Outbound Manipulations**).
2. Configure the rules according to your setup.

The following table shows an example of configured IP-to-IP outbound manipulation rules for calls between the Zoom Phone Cloud System IP Group and Generic SIP Trunk IP Group:

Rule Index	Description
0	Calls from SIP Trunk IP Group to Zoom Phone Cloud IP Group with the prefix destination number "+", do nothing.
1	Calls from SIP Trunk IP Group to Zoom Phone Cloud IP Group with any destination number between 1 to 9, add "+" to the prefix of the destination number.

Configuring Message Manipulation Rules

This section describes how to configure SIP message manipulation rules. SIP message manipulation rules can include insertion, removal, and/or modification of SIP headers. Manipulation rules are grouped into Manipulation Sets, enabling you to **Apply** multiple rules to the same SIP message (IP entity).

Once you have configured the SIP message manipulation rules, you need to assign them to the relevant IP Group (in the IP Group table) and determine whether they must be applied to inbound or outbound messages.

➢ **To configure SIP message manipulation rule for Zoom Phone Cloud System:**

1. Open the Message Manipulations page (**Setup** menu > **Signaling & Media** tab > **Message Manipulation** folder > **Message Manipulations**).
2. Configure a new manipulation rule (Manipulation Set 2) for Zoom Phone Cloud IP Group. This rule applies to OPTIONS messages sent to the Zoom Phone Cloud IP Group. This replaces the host part of the SIP Request-URI Header with the destination (Zoom Phone DC Server) IP address.

Parameter	Value
Index	0
Name	Zoom-Options (arbitrary name)
Manipulation Set ID	2

Parameter	Value
Message Type	**Options.Request**
Action Subject	**Header.Request-URI.URL.Host**
Action Type	**Modify**
Action Value	**Param.Message.Address.Dst.IP**

3. Configure another manipulation rule (Manipulation Set 1) for Zoom Phone Cloud IP Group. This rule applies to messages received from the Zoom Phone Cloud IP Group.This rule performs normalization of the messages received from Zoom Phone Cloud System.

Parameter	Value
Index	1
Name	Normalization
Manipulation Set ID	1
Message Type	**Any.Request**
Action Subject	**Message**
Action Type	**Normalize**

4. Assign Manipulation Set IDs 1 and 2 to the Zoom Phone Cloud IP Group:
   a. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
   b. Select the row of the Zoom Cloud IP Group, and then click **Edit**.
   c. Set the 'Inbound Message Manipulation Set' field to 1.
   d. Set the 'Outbound Message Manipulation Set' field to 2.
   e. Click **Apply**.

In your implementation, connectivity to the SIP Trunk may require additional message manipulation rules. Refer to the appropriate SIP Trunk Implementation Guide or contact an AudioCodes representative to order Professional Services from AudioCodes, and our Professional Services team will help you with your configuration.

Configuring Registration Accounts (Optional)

This section describes how to configure SIP registration accounts. This is required so that the SBC can register with the Generic SIP Trunk on behalf of the Zoom Phone Cloud systems. The Generic SIP Trunk requires registration and authentication to provide service.

In the typical deployment topology, the Served IP Group is the ZPLS module and Zoom Phone Cloud IP Groups and the Serving IP Group is Generic SIP Trunk IP Group.

Configure Registration Account only if this is required by SIP Trunk.

➢ **To configure a registration account:**

1. Open the Accounts table (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Accounts**).
2. Click **New** and configure the account for the ZPLS module IP Group according to the provided information, for example:

Parameter	Value
Served IP Group	ZPLS
Application Type	SBC
Serving IP Group	**SIPTrunk**
Host Name	As provided by the SIP Trunk provider
Register	**Regular**
Contact User	Trunk main line as provided by the SIP Trunk provider
Username	As provided by the SIP Trunk provider
Password	As provided by the SIP Trunk provider

3. Click **Apply**.
4. Click **New** and configure the account for Zoom DCs IP Group according to the provided information, for example:

Parameter	Value
Served IP Group	Zoom Cloud
Application Type	SBC

Parameter	Value
Serving IP Group	**SIPTrunk**
Host Name	As provided by the SIP Trunk provider
Register	**Regular**
Contact User	Trunk main line as provided by the SIP Trunk provider
Username	As provided by the SIP Trunk provider
Password	As provided by the SIP Trunk provider

5. Click **Apply**.

Configuring Firewall Settings (Optional)

As an additional security measure, there is an option to configure traffic filtering rules (access list) for incoming traffic on AudioCodes SBC. For each packet received on the configured network interface, the SBC searches the table from top to bottom until the first matching rule is found. The matched rule can permit (allow) or deny (block) the packet. Once a rule in the table is located, subsequent rules further down the table are ignored. If the end of the table is reached without a match, the packet is accepted. Please note that the firewall is stateless. The blocking rules **Apply** to all incoming packets, including UDP or TCP responses.

➢ **To configure a firewall rule:**

1. Open the Firewall table (**Setup** menu > **IP Network** tab > **Security** folder> **Firewall**).
2. Configure the following Access list rules for WAN IP Interface, based on the list of Zoom Phone System Servers:

Table 7-12: Firewall Table Rules

Index	Source IP	Subnet Prefix	Start Port	End Port	Protocol	Use Specific Interface	Interface ID	Allow Type
0	<Public DNS Server IP> (e.g., 8.8.8.8)	32	0	65535	Any	Enable	WAN_IF	Allow
1	162.12.233.59	32	0	65535	TCP	Enable	WAN_IF	Allow
2	162.12.232.59	32	0	65535	TCP	Enable	WAN_IF	Allow

Index	Source IP	Subnet Prefix	Start Port	End Port	Protocol	Use Specific Interface	Interface ID	Allow Type
3	162.12.235.85	32	0	65535	TCP	Enable	WAN_IF	Allow
4	213.19.144.198	32	0	65535	TCP	Enable	WAN_IF	Allow
5	213.244.140.198	32	0	65535	TCP	Enable	WAN_IF	Allow
6	103.122.166.248	32	0	65535	TCP	Enable	WAN_IF	Allow
7	103.122.167.248	32	0	65535	TCP	Enable	WAN_IF	Allow
8	209.9.211.198	32	0	65535	TCP	Enable	WAN_IF	Allow
9	207.226.132.198	32	0	65535	TCP	Enable	WAN_IF	Allow
10	64.211.144.247	32	0	65535	TCP	Enable	WAN_IF	Allow
11	<SIP Trunk IP address>	32	0	65535	TCP	Enable	WAN_IF	Allow
49	0.0.0.0	0	0	65535	Any	Enable	WAN_IF	Block

If in your configuration, connectivity to SIP Trunk (or other entities) is performed through the same IP Interface as Zoom Phone Cloud system (WAN_IF in our example), you must add rules to allow traffic from these entities. See an example in the row of index 11.

Configuring PSTN Breakout (Optional)

This section describes how to configure AudioCodes Mediant 800C SBC for connecting to PSTN network. This solution can be used for PSTN breakout when connectivity between SBC and SIP Trunk is also dropped, but there is a PSTN connection to the Telephony services.

As configuration settings of Gateway functionality (especially PSTN interface) may vary widely between customers, this document describes an example configuration. However, if you need assistance in your Gateway configuration and you have a valid support agreement with AudioCodes, please contact AudioCodes Professional Services (who also perform PoC testing, if required).

Configuring TDM Bus Clock Settings

This section describes the configuration of the TDM and clock timing parameters. In a traditional TDM service network such as PSTN, both ends of the TDM connection must be synchronized. If synchronization is not achieved, voice frames are either dropped (to prevent a buffer overflow condition) or inserted (to prevent an underflow condition). In both cases, connection quality and reliability are affected.

AudioCodes Gateway can be configured to recover clock from the PSTN line or to act as clock source to PSTN line (internal clock).

➢ **To configure synchronization based on clock from PSTN line:**

1. Open the TDM Bus Settings page (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **TDM Bus Settings**).
2. From the 'TDM Bus Clock Source' drop-down list, select **Network** to recover the clock from the line interface.
3. In the 'TDM Bus Local Reference' field, enter the trunk from which the clock is derived.

The E1/T1 trunk should recover the clock from the remote side (see below description of the 'Clock Master' parameter).

4. Enable automatic switchover to the next available "slave" trunk if the device detects that the local-reference trunk is no longer capable of supplying the clock to the system:
   a. From the 'TDM Bus PSTN Auto FallBack Clock' drop-down list, select Enable.
   b. From the 'TDM Bus PSTN Auto Clock Reverting' drop-down list, select Enable to enable the device to switch back to a previous trunk that returns to service if it has higher switchover priority.
5. Configure the PSTN trunk to recover/derive clock from/to the remote side of the PSTN trunk (i.e., clock slave or clock master): In the Trunk Settings page, configure the 'Clock Master' parameter to one of the following:
   - **Recovered** - to recover clock (i.e., slave)
   - **Generated** - to transmit clock (i.e., master)

Configuring Trunk Settings

This section describes the configuration of the PSTN Trunk parameters. This includes selecting the PSTN protocol and configuring related parameters.

➢ **To configure Trunk settings:**

1. Open the Trunk Settings page (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Trunks & Groups** > **Trunks**).
2. Select the trunk that you want to configure by clicking the required trunk number icon.
3. To configure a new trunk:
   - Configure the trunk parameters as required.
   - Click the **Apply** Trunk Settings button.


The trunk parameters should be configured according to the remote side.

4. The most commonly used parameters, which you need to configure are the protocol type (e.g., E1 Euro ISDN), the clock master of the trunk (Recovered/Generated), and the ISDN Termination Side (User/Network side).

Configuring Trunk Groups

This section describes the Trunk Groups configuration. A Trunk Group is a logical group of physical trunks and channels. A Trunk Group can include multiple trunks and a range of channels. To enable and activate the channels, you need to configure the Trunk Group and assign it telephone numbers. Channels that are not configured in this table are disabled. Once you have configured your Trunk Group, you can use it for call routing.

➢ **To configure a Trunk Group:**

1. Open the Trunk Settings page (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Trunks & Groups** > **Trunk Groups**).
2. Configure Trunk Group as shown in the following table:

Table 7-13: Example of the Trunk Group Configuration

Group Index	Module	From Trunk	To Trunk	Channels	Phone Number	Trunk Group ID	Tel Profile Name
1	Module 1 PRI	1	1	1-31	-	1	None


This is just example; your configuration can be different.

3. Click **Apply**

Configuring Trunk Group Settings

This section describes the Trunk Group Settings table, which lets you configure various settings per Trunk Group, configured in the previous section. The main configuration includes channel select method, which defines how the device allocates incoming IP-to-Tel calls to the channels of a Trunk Group.

➢ **To configure Trunk Group Settings:**

1. Open the Trunk Settings page (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Trunks & Groups** > **Trunk Group Settings**).
2. Configure Trunk Group Settings as shown in the following table:

Table 7-14: Example of the Trunk Group Settings

Index	Name	Trunk Group ID	Channel Select Mode
0	PSTN Breakout	1	**Channel Cyclic Ascending**
All other parameters can be left unchanged with their default values.			

This is just example; your configuration can be different.

3. Click **Apply**.

Configuring IP-to-Tel Routing Rule

This section describes the Gateway IP to PSTN Routing settings. For call routing from the ZPLS to the PSTN trunk, you need to configure an **IP-to-Tel Routing** rule. In other words, you need to route calls from the IP Group of the ZPLS to the Trunk Group that you configured for the PSTN trunk (i.e., ID 1) in Configuring Trunk Groups on the previous page.

➢ **To configure an IP-to-Tel Routing rule:**

1. Open the **IP-to-Tel Routing** page (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Routing**> **IP-to-Tel Routing**).
2. Configure **IP-to-Tel Routing** rule as shown in the following table:

Table 7-15: Example of the IP-to-Tel Routing Rule Configuration

Index	Name	Destination Phone Prefix	Destination Type	Trunk Group ID
0	PSTN Breakout (arbitrary	*	**Trunk Group**	1

Index	Name	Destination Phone Prefix	Destination Type	Trunk Group ID
	name)			
All other parameters can be left unchanged with their default values.				

The asterisk (*) value of the 'Destination Phone Prefix' parameter denotes all dialed calls.

3. Click **Apply**.

Configuring Tel-to-IP Routing Rule

This section describes the Gateway PSTN to IP Routing settings. To receive calls from the PSTN network, you need to add rules to route calls received from the E1 trunk (e.g., Trunk Group ID 1) to the ZPLS module.

➢ **To configure a Tel-to-IP routing rule:**

1. Open the Tel-to-IP Routing page (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Routing** > **Tel-to-IP Routing**).
2. Configure Tel-to-IP Routing Rules as shown in the following table:

Table 7-16: Example of the Tel-to-IP Routing Rules Configuration

Index	Name	Source Trunk Group ID	Destination IP Group
0	PSTN to ZPLS (arbitrary name)	1	ZPLS
All other parameters can be left unchanged with their default values.			

3. Click **Apply**.

Adapt SBC Routing Table with Local PSTN Breakout

This section describes how to change SBC routing rules to route calls from the ZPLS to the local PSTN. The following IP-to-IP routing rule needs to be added for this purpose.

➢ **To configure IP-to-IP routing rule:**

1. Open the IP-to-IP Routing table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **IP-to-IP Routing**).
2. **Add** following routing rule at the end of the table:

Table 7-17: Configuration IP-to-IP Routing Rules with local PSTN Breakout

Index	Name	Alternative Route Options	Source IP Group	Request Type	Dest Type
5	ZPLS to PSTN (arbitrary name)	Alternative Route Ignore Inputs	ZPLS	INVITE	Gateway

Miscellaneous Configuration

This section describes miscellaneous SBC configuration.

Configuring Mutual TLS Authentication for SIP

This section describes how to configure SBC to work in mutual (two-way) TLS authentication mode.

> This section is required only if implementation of MTLS connection with the Zoom Phone System is required and depends on enabling MTLS on the Zoom side.

➢ **To configure Mutual TLS authentication for SIP messaging with Zoom:**

1. Enable two-way authentication on the Zoom SIP Interface:

   In the SIP Interface table, assign Zoom TLS context to the Zoom SIP Interface and configure the 'TLS Mutual Authentication' parameter to **Enable**.
2. Make sure that the TLS certificate is signed by a CA.
3. Make sure that CA certificates are imported into the Trusted Root Certificates table.

To further enhance security, it's possible to configure the SBC to verify the server certificates, when it acts as a client for the TLS connection.

➢ **To configure SBC to verify Server certificate:**

1. Open the SBC Security Settings page (**Setup** menu > **IP Network** tab > **Security** folder > **Security Settings**).
2. From the 'TLS Client Verify Server Certificate' drop-down list, select **Enable**.
3. Click **Apply**.

8 Zoom Data Centers

Connectivity to the Zoom Phone System signaling via Fully Qualified Domain Names (FQDN) depends on the geographical location of the customer SBC(s) and the corresponding Zoom Data Center that the customer would like to send and receive traffic. Zoom Phone Cloud System options are currently available in four separate regions across the globe: North America, Europe, APAC and Australia.

Table 8-1: Regional instances resolve to the following IP addresses

Region	Traffic Type	Protocol	Ports	A Record	IP Address
North America	Signaling	TCP/TLS	5061	us01peer01.sc.zoom.us	162.12.233.59
	Signaling	TCP/TLS	5061	us01peer01.ny.zoom.us	162.12.232.59
	Signaling	TCP/TLS	5061	us01peer01.dv.zoom.us	162.12.235.85
EMEA	Signaling	TCP/TLS	5061	us01peer01.am.zoom.us	213.19.144.198
	Signaling	TCP/TLS	5061	us01peer01.fr.zoom.us	213.244.140.198
Australia	Signaling	TCP/TLS	5061	us01peer01.sy.zoom.us	103.122.166.248
	Signaling	TCP/TLS	5061	us01peer01.me.zoom.us	103.122.167.248
APAC	Signaling	TCP/TLS	5061	us01peer01.hk.zoom.us	209.9.211.198
	Signaling	TCP/TLS	5061	us01peer01.ty.zoom.us	207.226.132.198
South America	Signaling	TCP/TLS	5061	us01peer01.sp.zoom.us	64.211.144.247

Table 8-2: Regional Media Traffic and Ports

Region	Traffic Type	Protocol	Ports	Destination
North America	Media	UDP/SRTP	20000-64000	162.12.232.0/22
EMEA	Media	UDP/SRTP	20000-64000	213.19.144.0/24
	Media	UDP/SRTP	20000-64000	213.244.140.0/24
Australia	Media	UDP/SRTP	20000-64000	103.122.166.0/23
APAC	Media	UDP/SRTP	20000-64000	209.9.211.0/24
	Media	UDP/SRTP	20000-64000	207.226.132.0/24

9 Zoom Public Trusted Certificate List

The following table lists the Zoom Public Trusted Certificates.

Zoom Public Trusted Certificate List

Certificate Issuer Organization	Common Name or Certificate Name
Buypass AS-983163327	Buypass Class 2 Root CA
Buypass AS-983163327	Buypass Class 3 Root CA
Baltimore	Baltimore CyberTrust Root
Cybertrust, Inc	Cybertrust Global Root
DigiCert Inc	DigiCert Assured ID Root CA
DigiCert Inc	DigiCert Assured ID Root G2
DigiCert Inc	DigiCert Assured ID Root G3
DigiCert Inc	DigiCert Global Root CA
DigiCert Inc	DigiCert Global Root G2
DigiCert Inc	DigiCert Global Root G3
DigiCert Inc	DigiCert High Assurance EV Root CA
DigiCert Inc	DigiCert Trusted Root G4
GeoTrust Inc.	GeoTrust Global CA
GeoTrust Inc.	GeoTrust Primary Certification Authority
GeoTrust Inc.	GeoTrust Primary Certification Authority - G2
GeoTrust Inc.	GeoTrust Primary Certification Authority - G3
GeoTrust Inc.	GeoTrust Universal CA
GeoTrust Inc.	GeoTrust Universal CA 2
DigiCert Inc	DigiCert Global Root G3
Symantec Corporation	Symantec Class 1 Public Primary Certification Authority - G4

Certificate Issuer Organization	Common Name or Certificate Name
Symantec Corporation	Symantec Class 1 Public Primary Certification Authority - G6
Symantec Corporation	Symantec Class 2 Public Primary Certification Authority - G4
Symantec Corporation	Symantec Class 2 Public Primary Certification Authority - G6
Thawte, Inc.	Thawte Primary Root CA
Thawte, Inc.	Thawte Primary Root CA - G2
Thawte, Inc.	Thawte Primary Root CA - G3
VeriSign, Inc.	VeriSign Class 1 Public Primary Certification Authority - G3
VeriSign, Inc.	VeriSign Class 2 Public Primary Certification Authority - G3
VeriSign, Inc.	VeriSign Class 3 Public Primary Certification Authority - G3
VeriSign, Inc.	VeriSign Class 3 Public Primary Certification Authority - G4
VeriSign, Inc.	VeriSign Class 3 Public Primary Certification Authority - G5
VeriSign, Inc.	VeriSign Universal Root Certification Authority
AffirmTrust	AffirmTrust Commercial
AffirmTrust	AffirmTrust Networking
AffirmTrust	AffirmTrust Premium
AffirmTrust	AffirmTrust Premium ECC
Entrust, Inc.	Entrust Root Certification Authority
Entrust, Inc.	Entrust Root Certification Authority - EC1
Entrust, Inc.	Entrust Root Certification Authority - G2

Certificate Issuer Organization	Common Name or Certificate Name
Entrust, Inc.	Entrust Root Certification Authority - G4
Entrust.net	Entrust.net Certification Authority (2048)
GlobalSign	GlobalSign
GlobalSign	GlobalSign
GlobalSign	GlobalSign
GlobalSign nv-sa	GlobalSign Root CA
The GoDaddy Group, Inc.	Go Daddy Class 2 CA
GoDaddy.com, Inc.	Go Daddy Root Certificate Authority - G2
Starfield Technologies, Inc.	Starfield Class 2 CA
Starfield Technologies, Inc.	Starfield Root Certificate Authority - G2
QuoVadis Limited	QuoVadis Root CA 1 G3
QuoVadis Limited	QuoVadis Root CA 2
QuoVadis Limited	QuoVadis Root CA 2 G3
QuoVadis Limited	QuoVadis Root CA 3
QuoVadis Limited	QuoVadis Root CA 3 G3
QuoVadis Limited	QuoVadis Root Certification Authority
Comodo CA Limited	AAA Certificate Services
AddTrust AB	AddTrust Class 1 CA Root
AddTrust AB	AddTrust External CA Root
COMODO CA Limited	COMODO Certification Authority
COMODO CA Limited	COMODO ECC Certification Authority
COMODO CA Limited	COMODO RSA Certification Authority
The USERTRUST Network	USERTrust ECC Certification Authority
The USERTRUST Network	USERTrust RSA Certification Authority

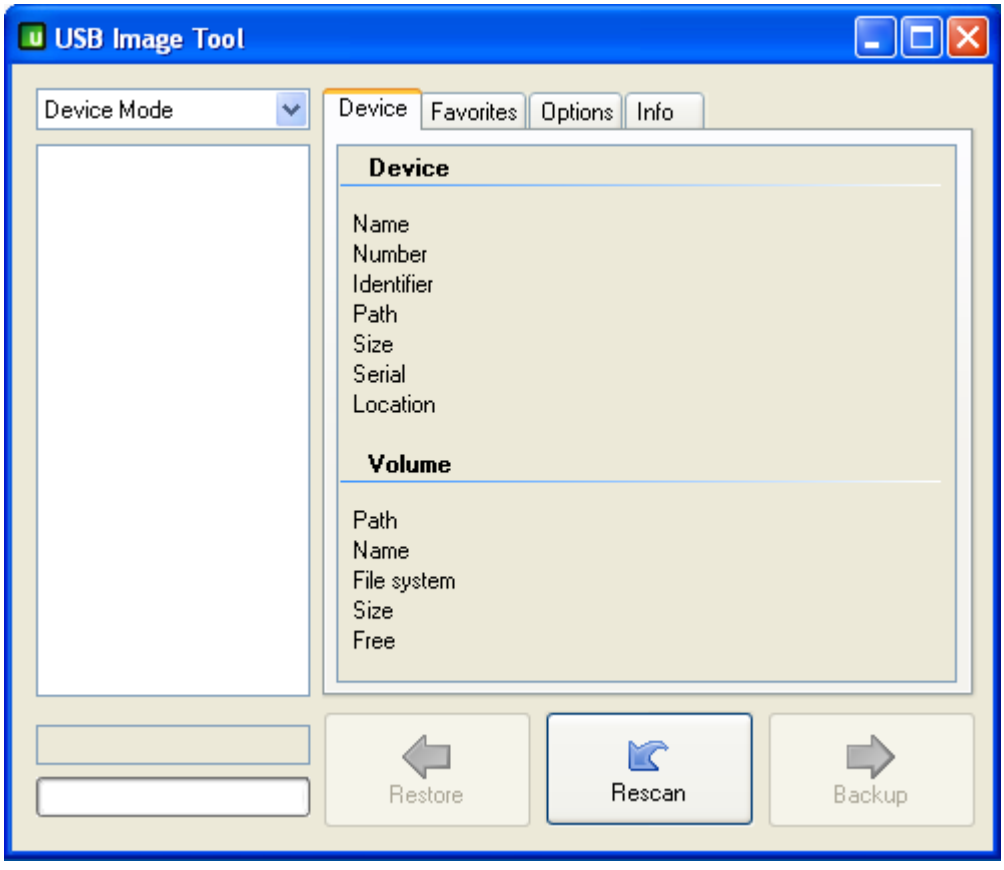
Certificate Issuer Organization	Common Name or Certificate Name
T-Systems Enterprise Services GmbH	T-TeleSec GlobalRoot Class 2
T-Systems Enterprise Services GmbH	T-TeleSec GlobalRoot Class 3

10 Recovering ZPLS from Disaster

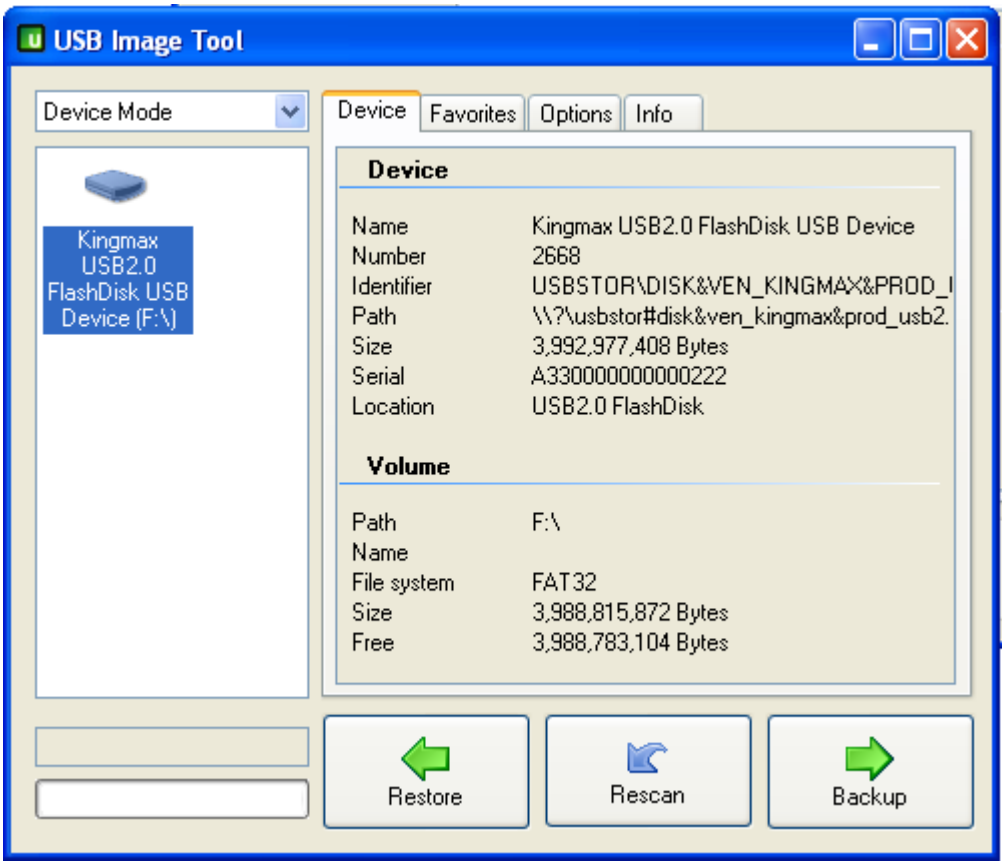
In case the ZPLS becomes unresponsive due to reasons like a faulty SSD, you can restore it using the provided USB dongle. The USB dongle is bootable and contains VMWare 7.0 running on a Linux OS, enabling you to perform the necessary recovery procedures.

➢ **To perform a recovery from disaster:**

1. Download the virtual OVA file from here. You need this file to build the ZPLS virtual server after you complete the recovery process.
2. (Optional) If you don't have the supplied USB dongle (for whatever reason), follow these steps to create a bootable USB, using the third-party, USB Image Tool program as an example. Pay attention that USB dongle has at least a 32 GB capacity.
   a. Download the VMware ESXi image file (.img) by clicking here, and then save it on a folder on your PC.
   b. Open a USB burn application (e.g., USB Image Tool):

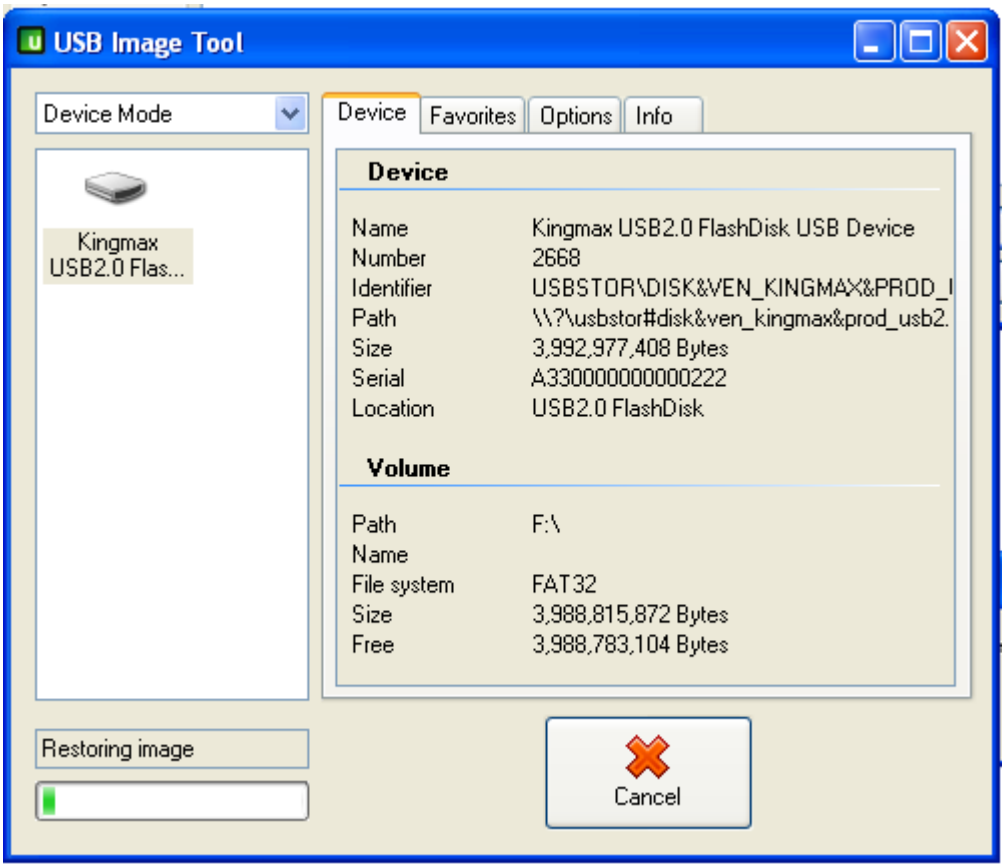


   c. Plug the USB dongle into the USB port on your PC where you saved your downloaded ESXi image file.
   d. Once the dongle is detected, select its' icon:



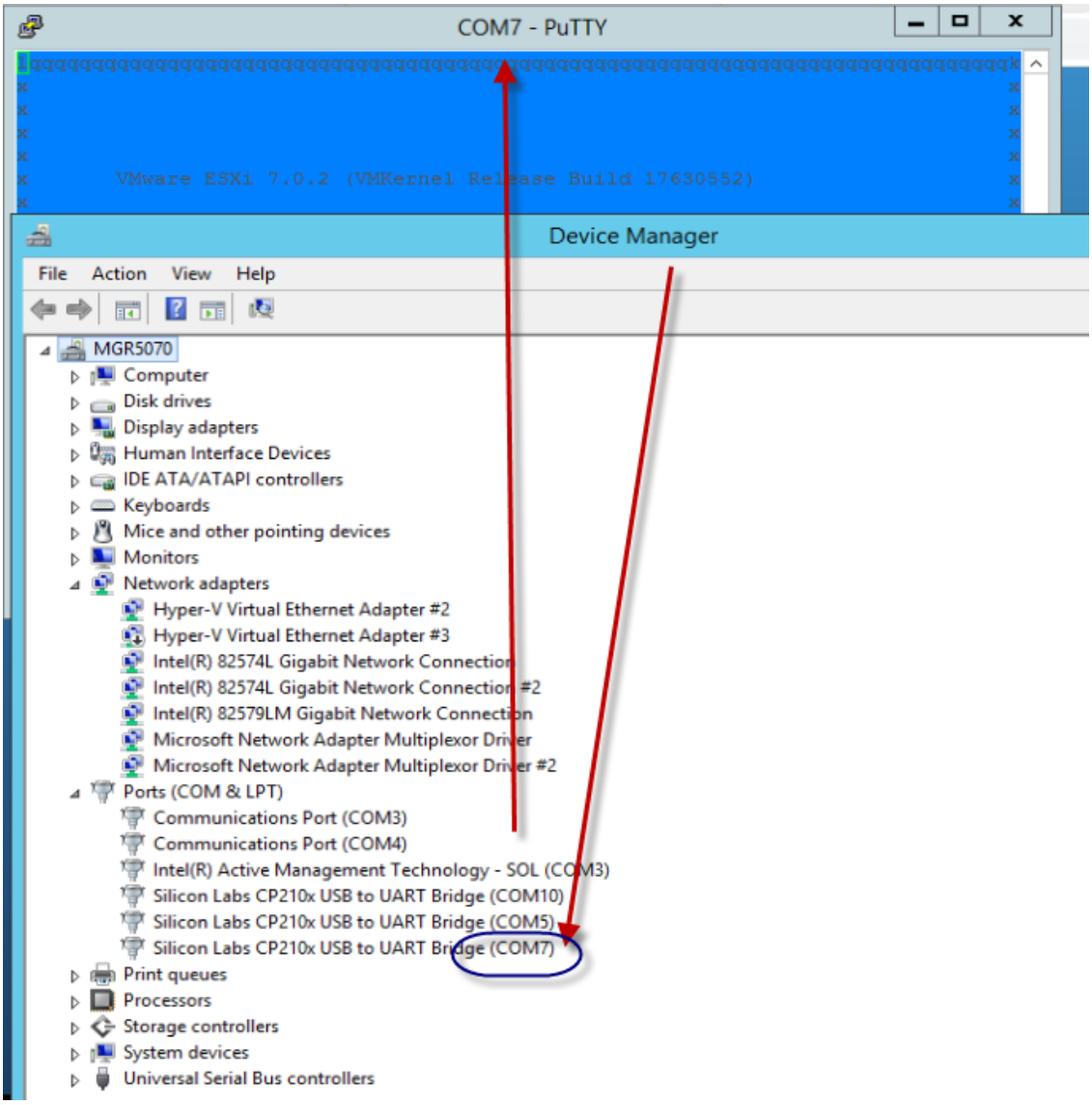
e. Click **Restore**, select the downloaded ESXi image file (.img), and then click **Open**; you are prompted to approve the restore action.

f. Click **Yes**; the restore process starts and the progress is displayed on the bottom-left side progress bar:

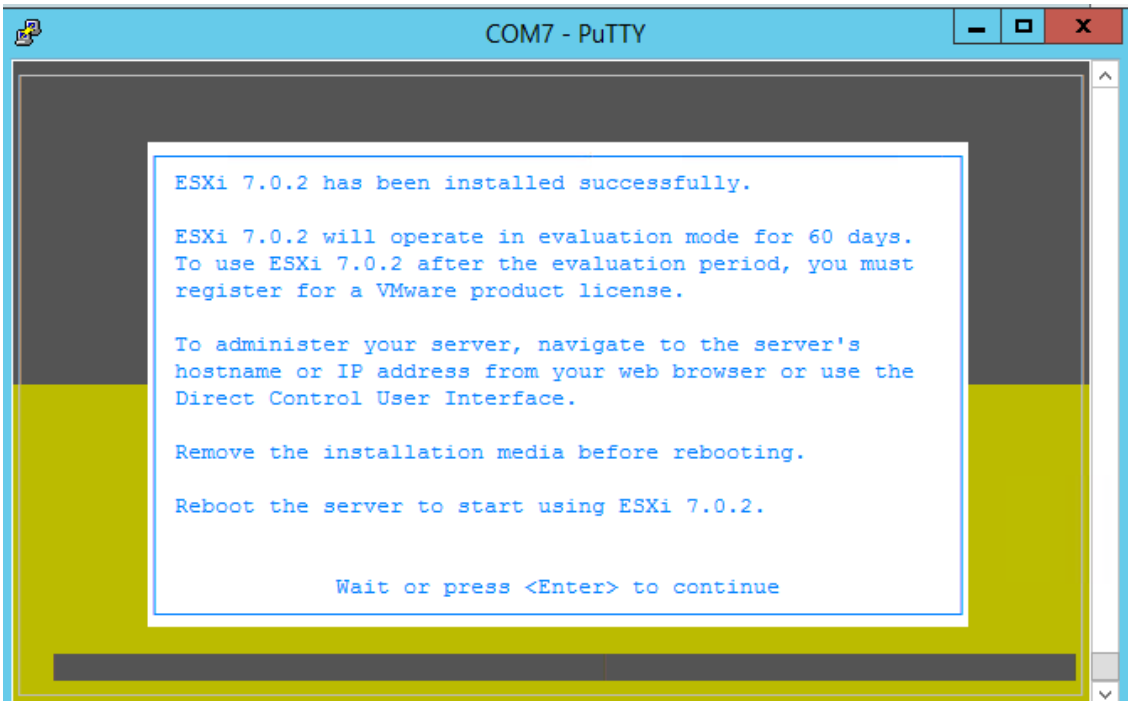


g. When the restore process finishes, perform a "Safely Remove Hardware" on your PC, and then unplug the USB dongle from the PC.

3. Use Windows Device Manager to determine the COM port (e.g., COM7) and connect your computer to the ZPLS (rear panel of the Mediant 800C), using a serial interface:

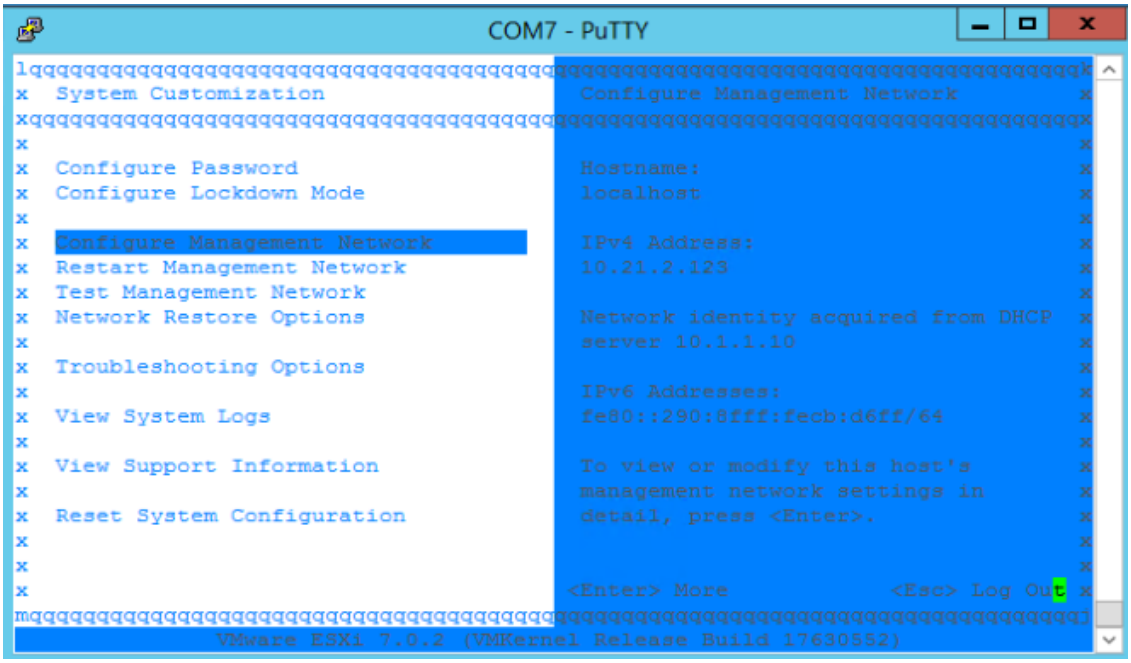


4. Connect the USB dongle to the ZPLS (USB port on rear panel of Mediant 800C) and do a cold restart (power off power on). Make sure that it boots from the USB dongle as first priority. Installation of the VMware ESXi image on the ZPLS begins (may take up to 15 minutes):

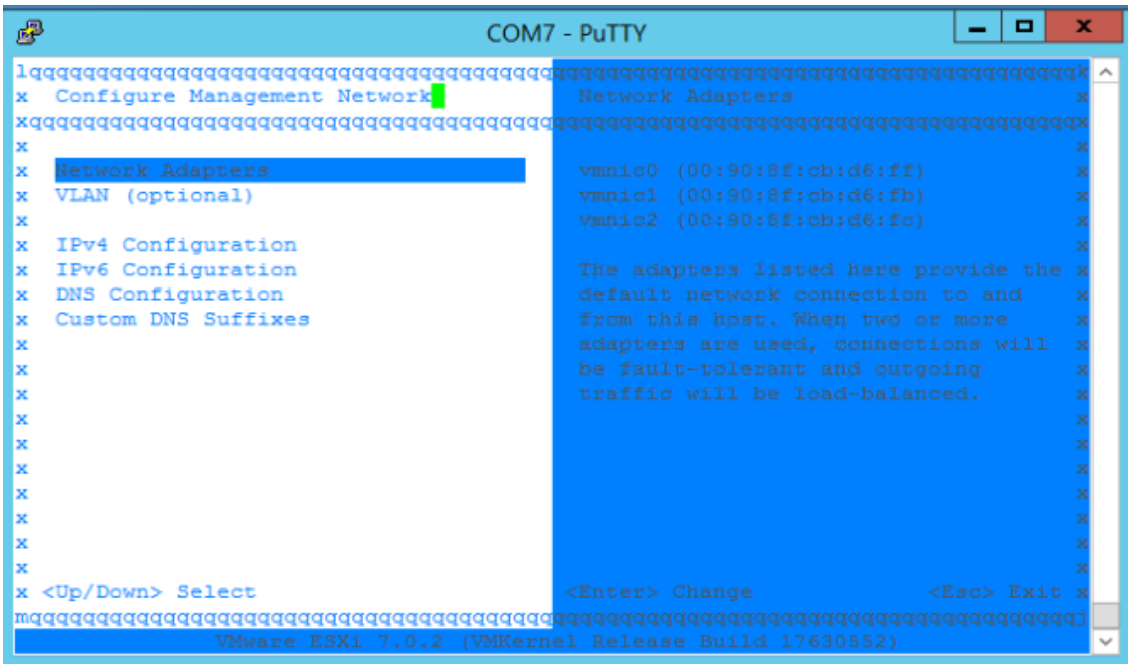


5. Remove the USB dongle, and then cold restart the ZPLS.
6. Configure the root's password to **Audc123!**.
7. Press F2 to customize settings (password and IP address):

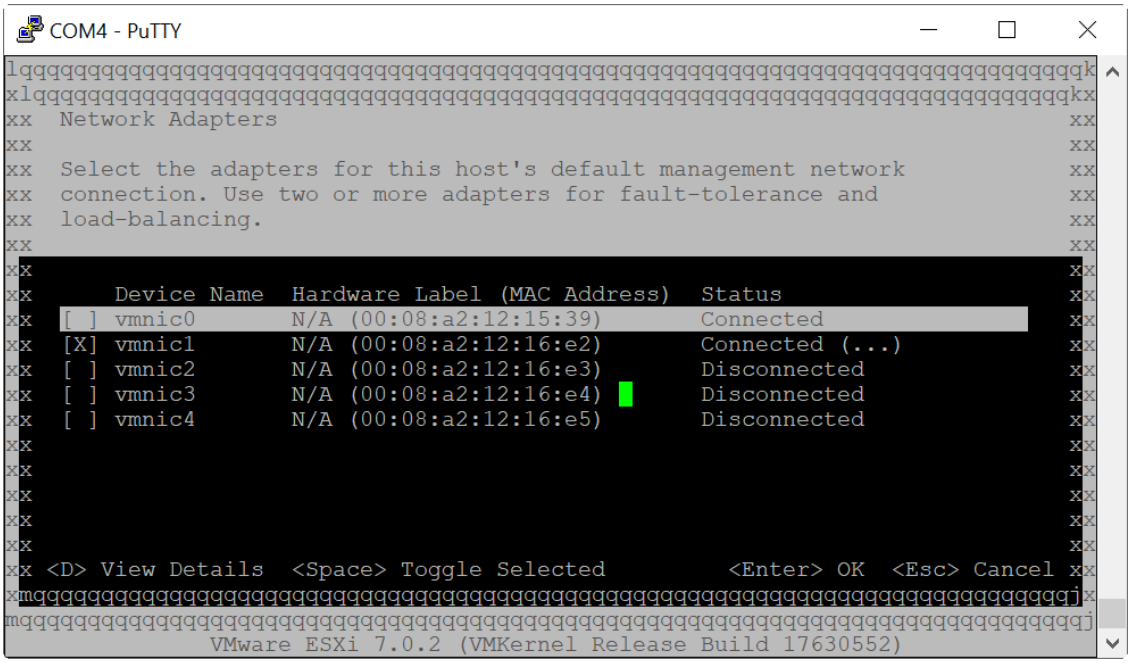
   a. Using the up/down arrow keys, select **Configure Management Network**, and then press Enter:



b. Navigate to the Network Adapters screen:

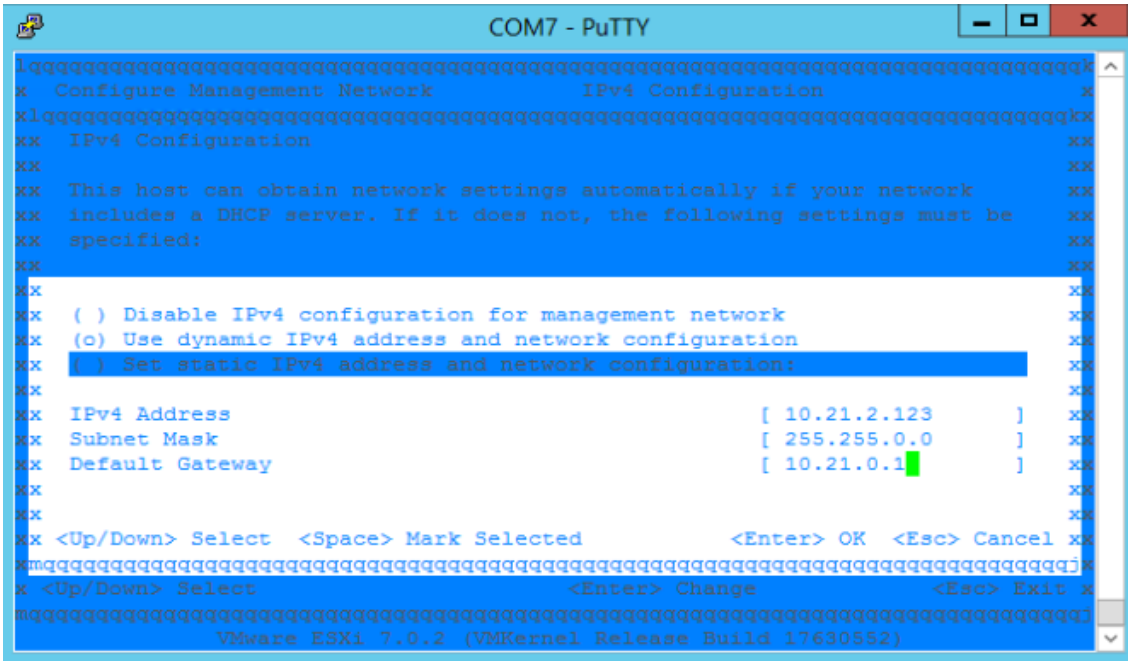


c. Using your keyboard's Spacebar, select vmnic1 network interface:

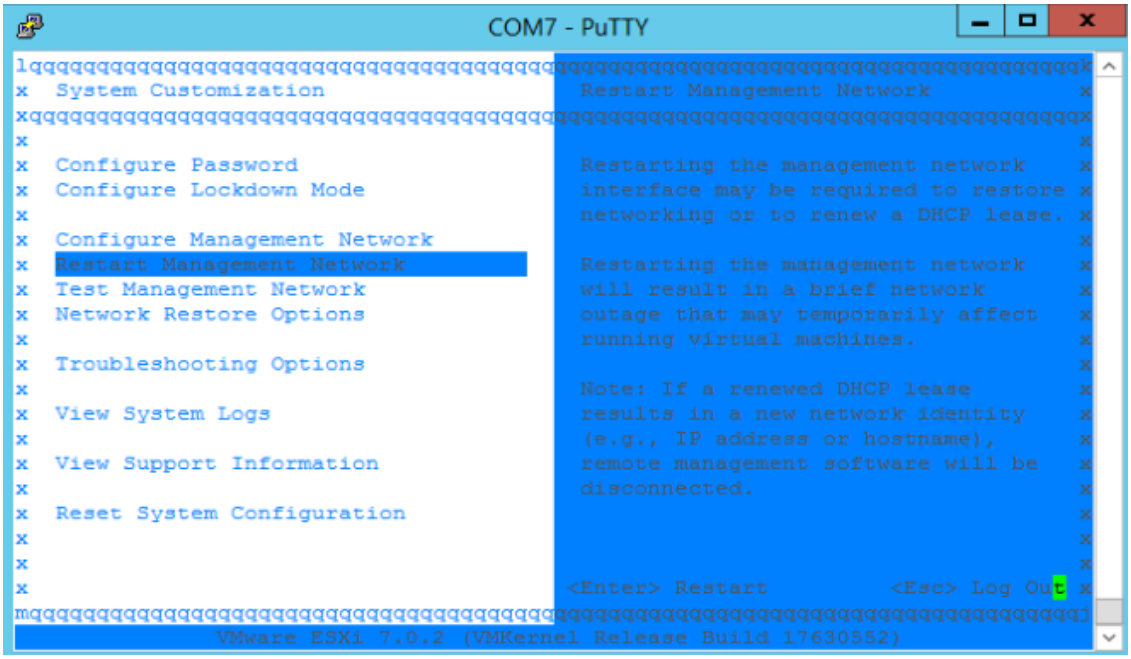


d. Press the Esc key, navigate to **IPv4 Configuration** > **Set Static IPv4 address** ...,

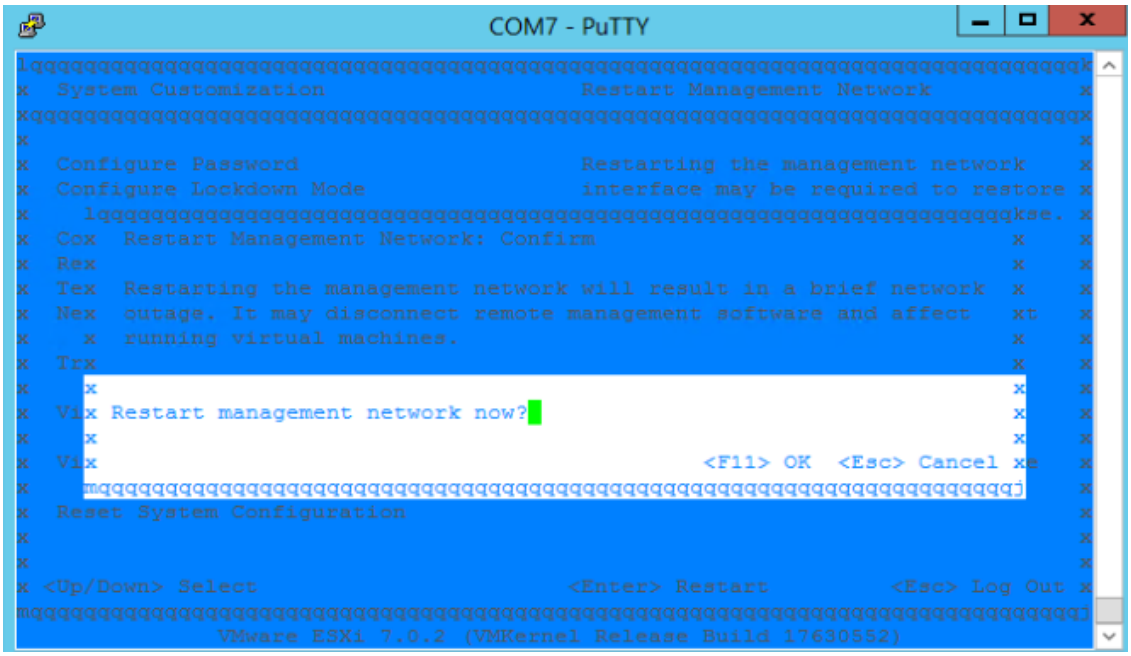
e. Configure the local IP address, subnet and default gateway:



f. Press the Esc key twice, and then navigate to **Restart Management Network**:



g. Press the F11 key to confirm and wait:

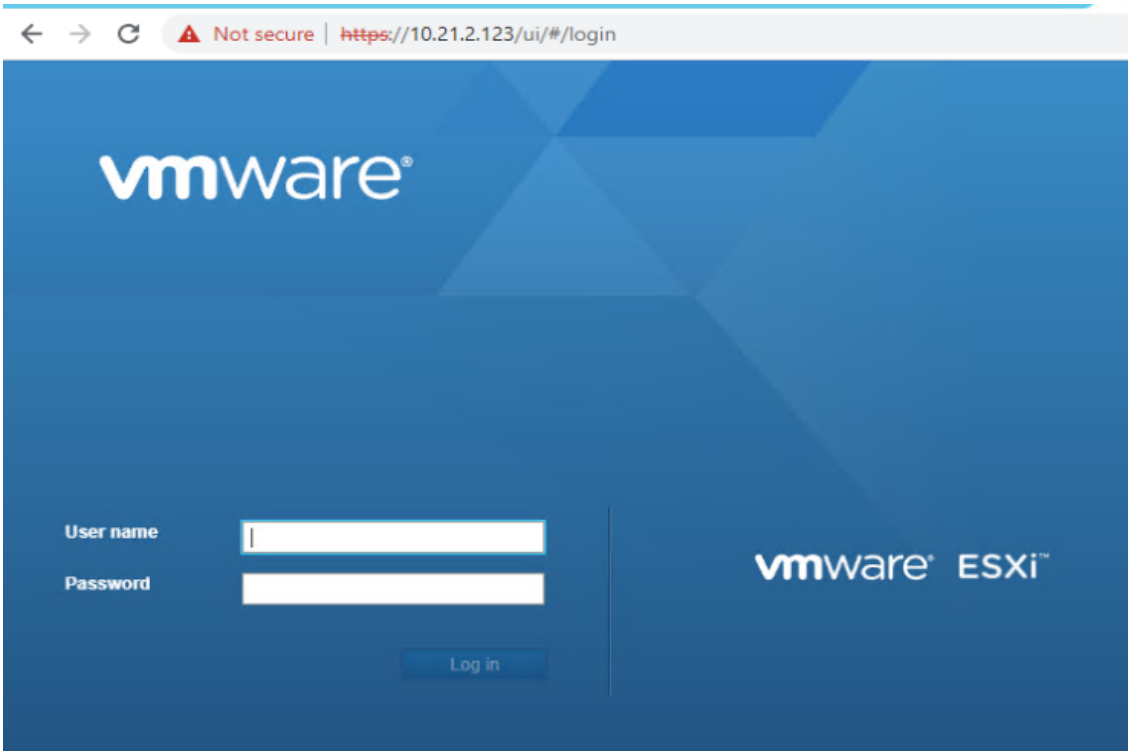


h. Press the Enter key to exit.

i. Press the Esc key, and then press the F12 key to restart the ZPLS.

8. Access the VMWare's web-based management interface:

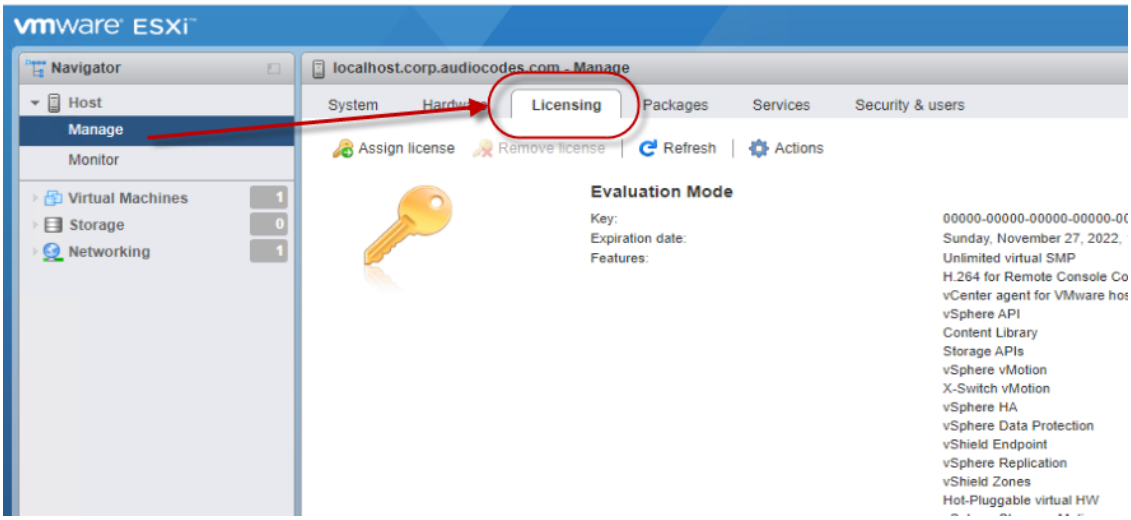
a. Open your web browser and browse to https://<local IP address configured above>/ui/#/login:



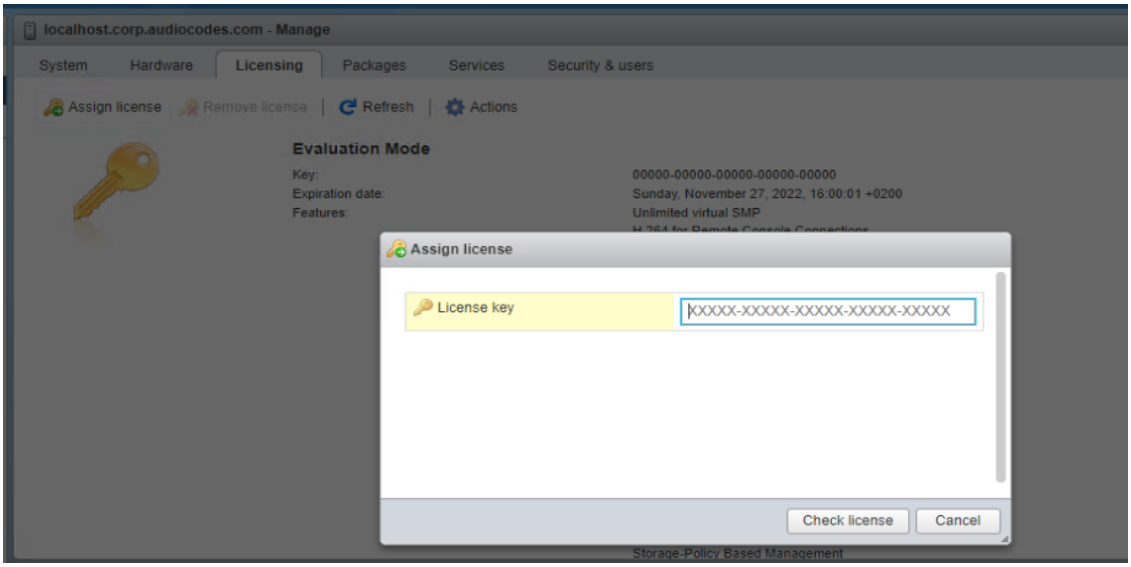
b. Log in using the same password that is used for accessing the ZPLS through serial (root's password).

9. Install the VMWare's license:

a. Navigate to **Manage**, and then select the **Licensing** tab:

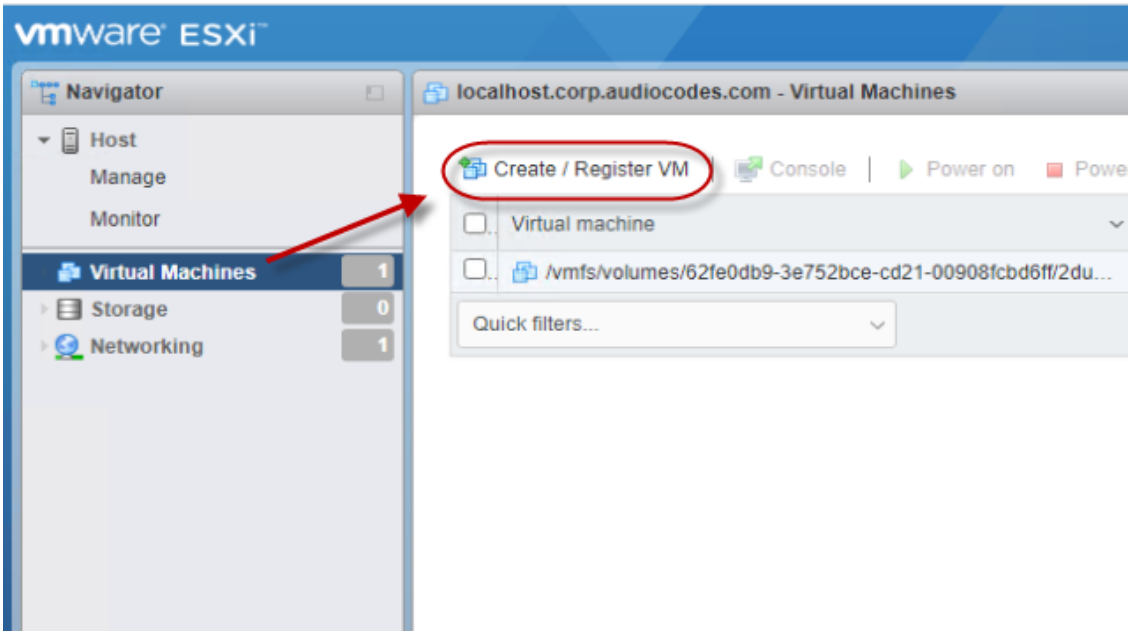


b. Click **Assign license**, and then in the opened dialog box, paste the key in the field:

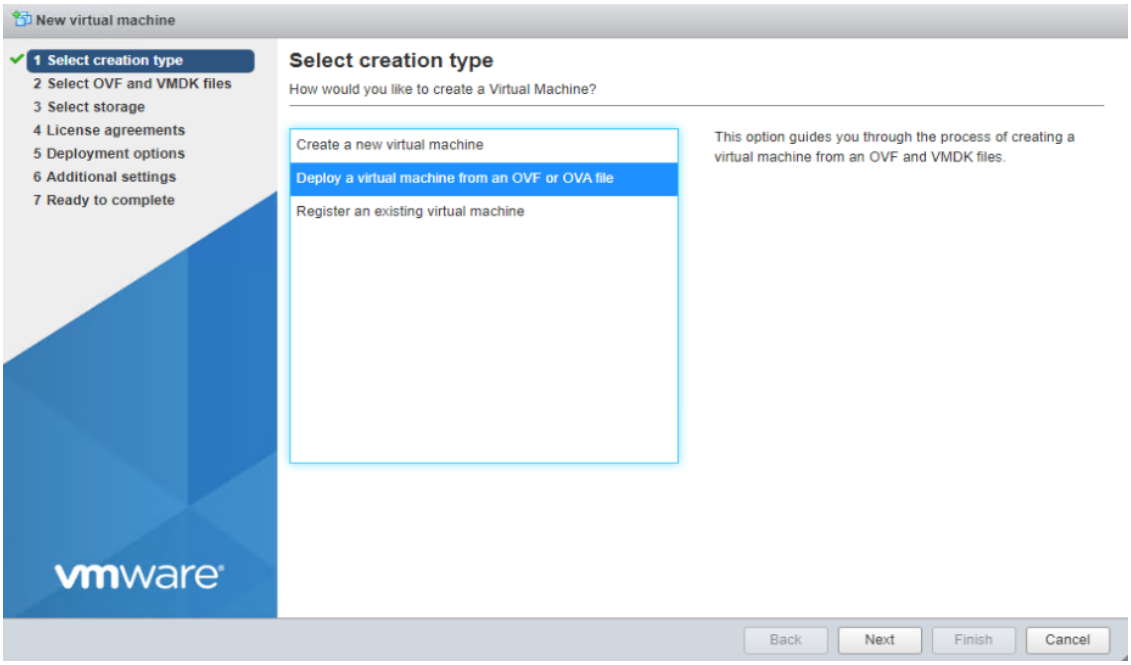


10. Create a virtual machine:

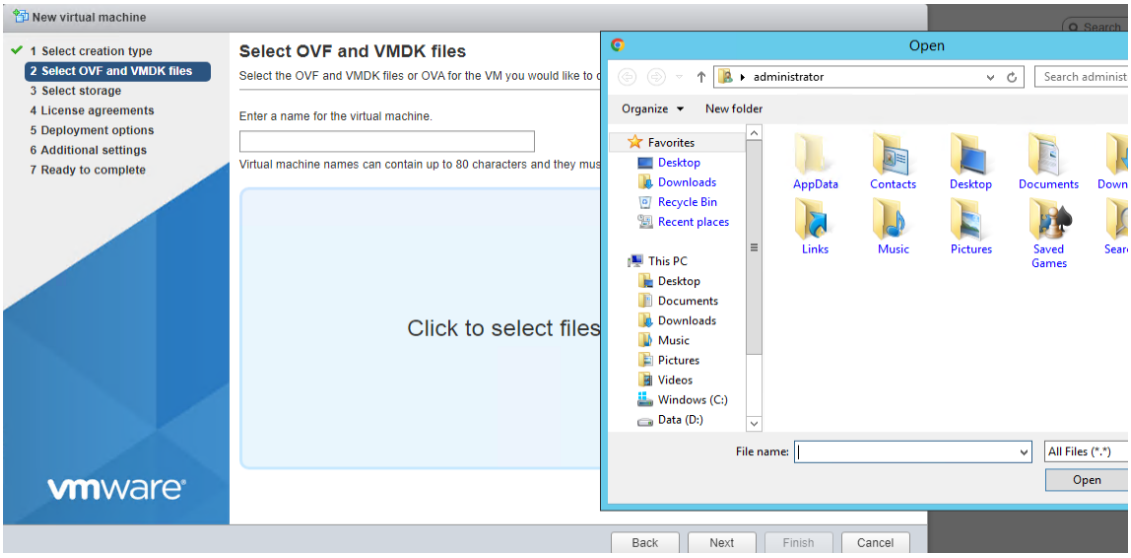
a. Navigate to **Virtual Machines**, and then click **Create** to open the wizard for creating a virtual machine:



b. **Select creation type:** Select the **Deploy a virtual machine from an OVF or OVA file** option, and then click **Next**:



c. **Select OVF and VMDK files:** Configure the server's name to "ZPLS", select the OVA file (or drag it on to the window), and then click **Next**:



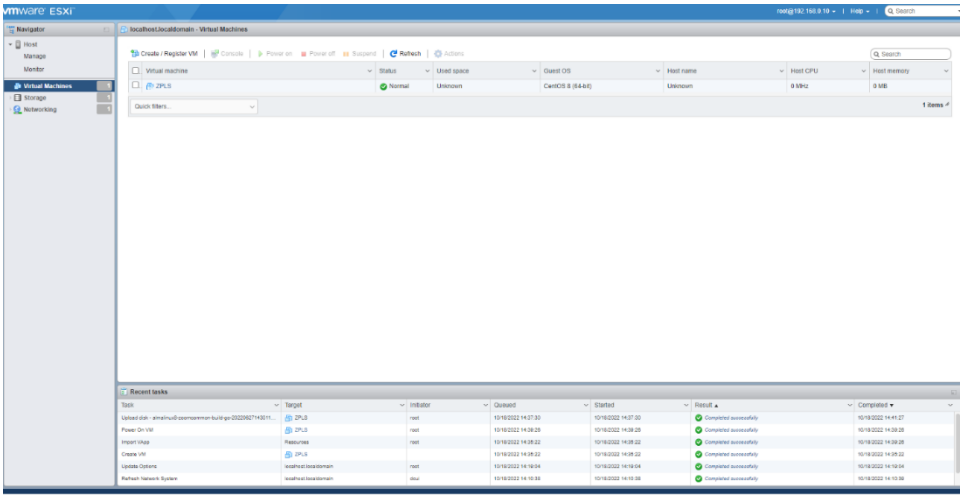
d. **Select storage:** Keep default settings, and then click **Next**.

e. **License agreements:** Agree to the license agreement, and then click **Next**.

f. **Deployment options:** Keep default settings, and then click **Next**.

g. **Additional settings:** Keep default settings, and then click **Next**.

h. Click **Finish**, and then wait until the new virtual machine is created:



i. Double-click the newly created virtual machine and check that the virtual machine is accessible from the configured IP address.

11 Enabling OSN's Internal vNIC

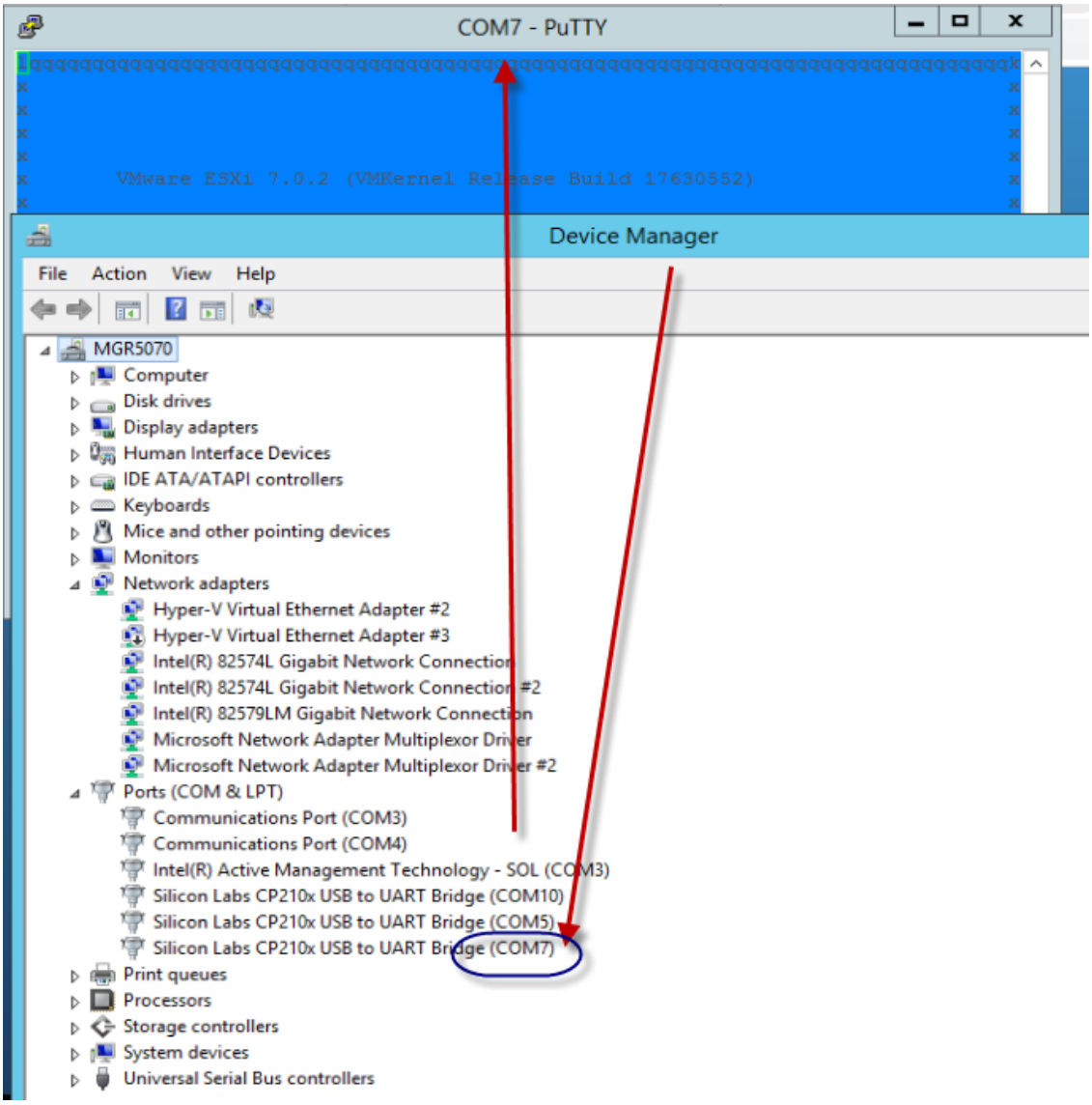
This section describes the procedure to enable the internal vNIC on the OSN module. This is required if a customer prefers to connect both the SBC and ZPLS applications to the network via a single Ethernet cable.

➢ **Prerequisites:**

- SBC is already installed and accessible with IP address at the same subnet as ZPLS.
- ZPLS is accessible through one of the 4 NICs, in order to remotely perform the required settings for the internal NIC.
- Serial connectivity to the OSN module of Mediant 800C.

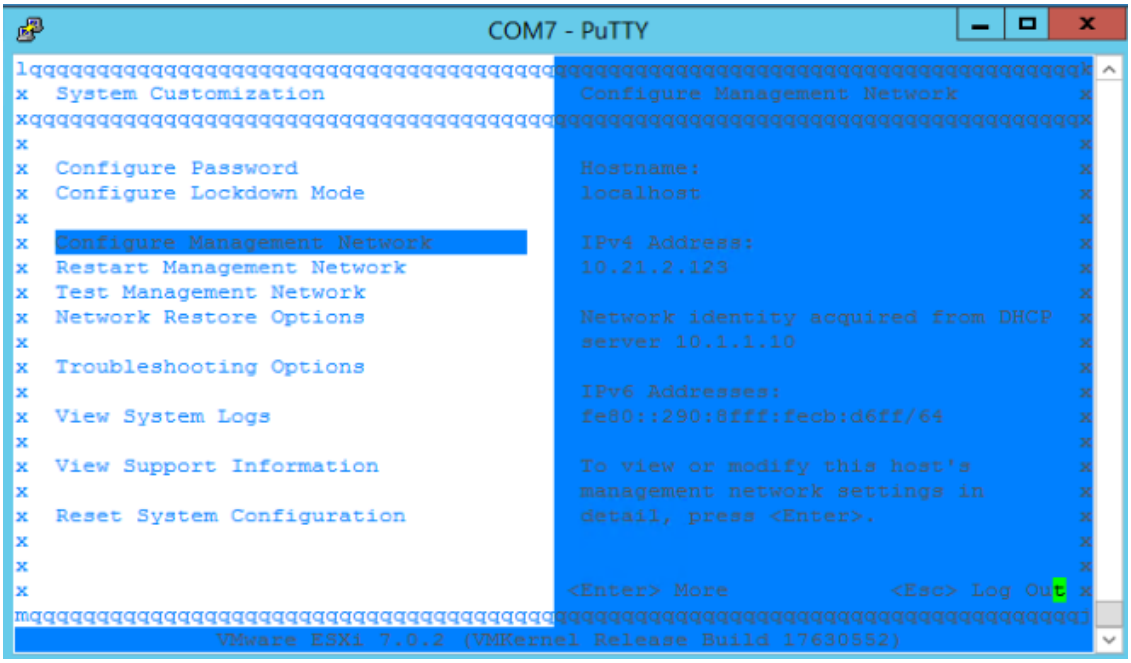
➢ **To enable OSN's internal vNIC:**

1. Use Windows Device Manager to determine the COM port (e.g., COM7) and connect your computer to the ZPLS (rear panel of the Mediant 800C), using a serial interface:

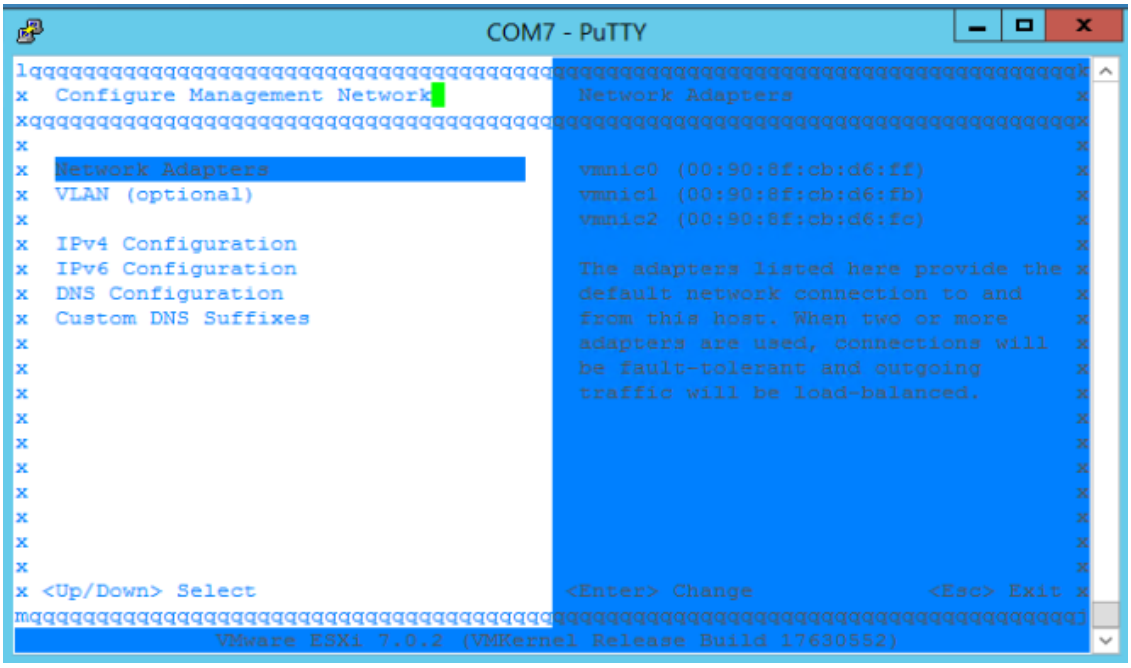


2. Access menu using the root's password (**Audc123!**).
3. Press F2 to customize settings.

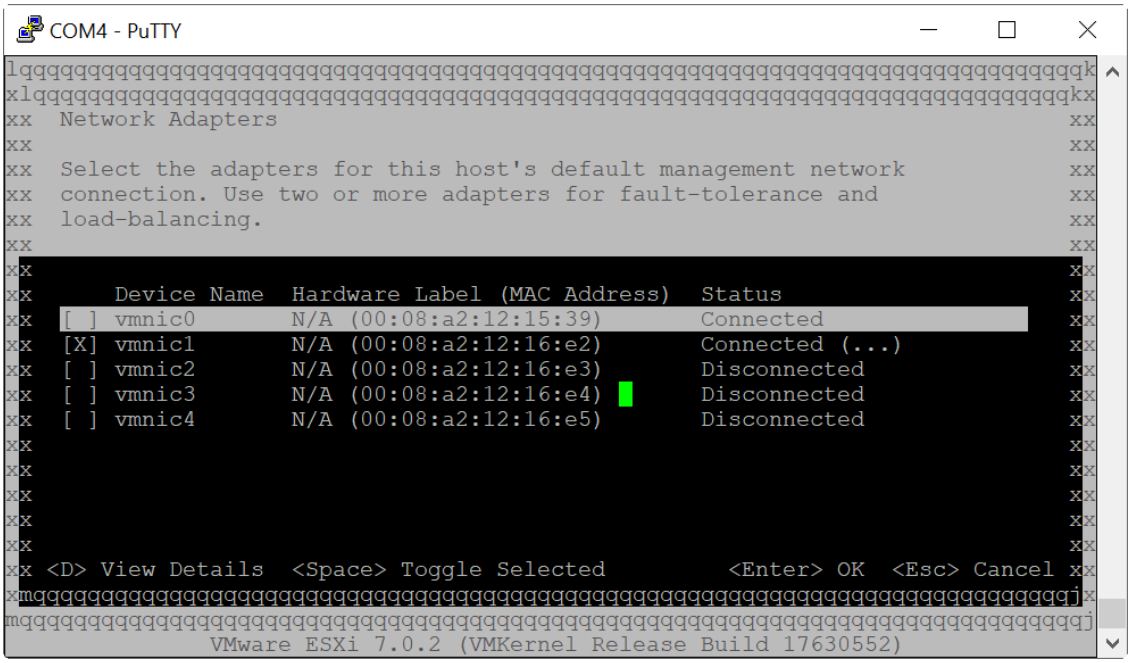
a. Using the up/down arrow keys, select **Configure Management Network**, and then press Enter.



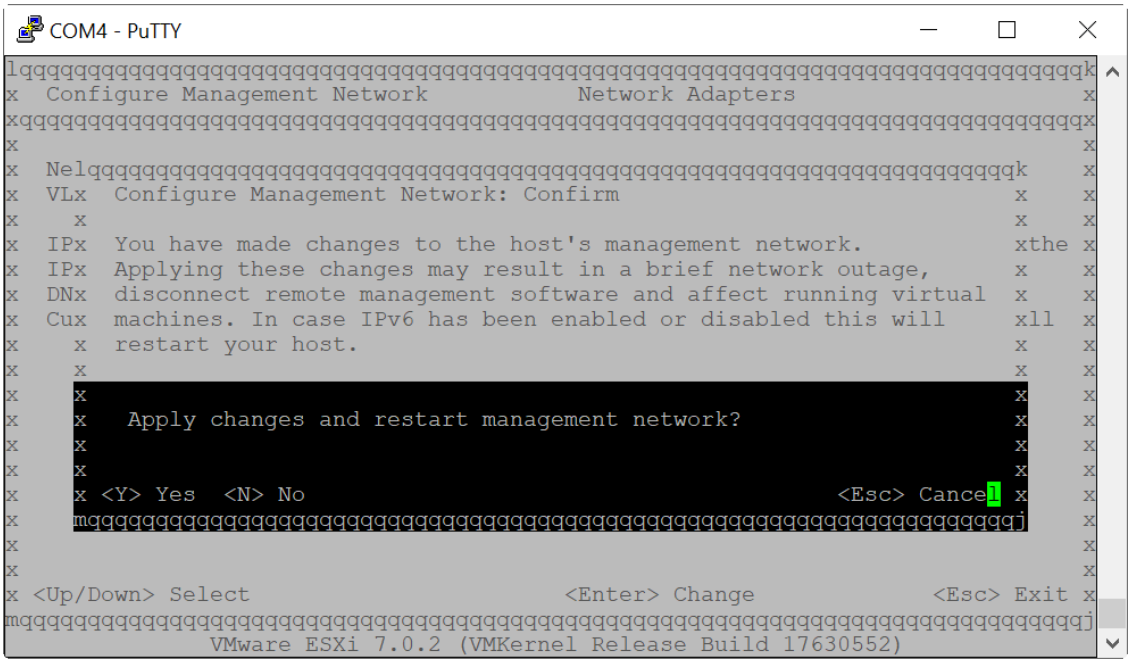
b. Navigate to the **Network Adapters** screen:



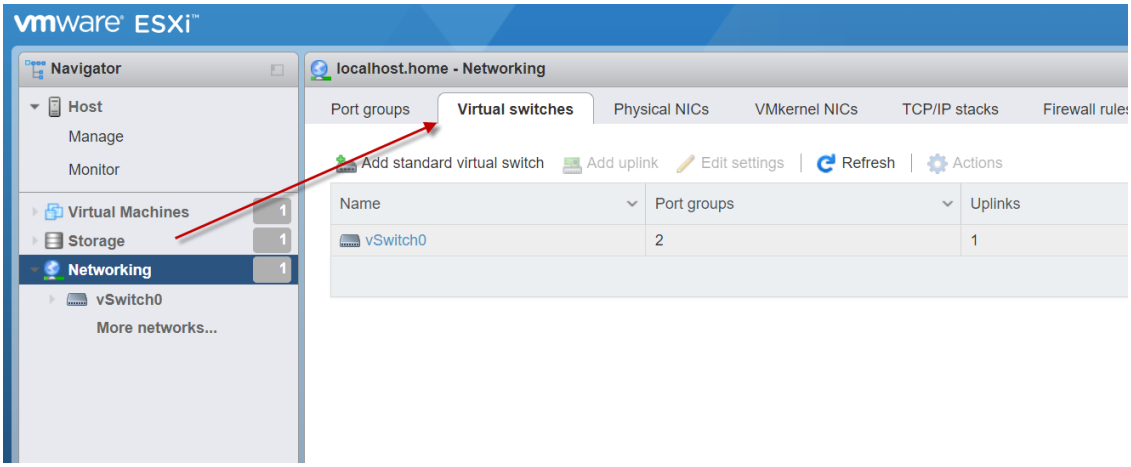
c. Using your keyboard's Spacebar, select **vmnic0** network interface.



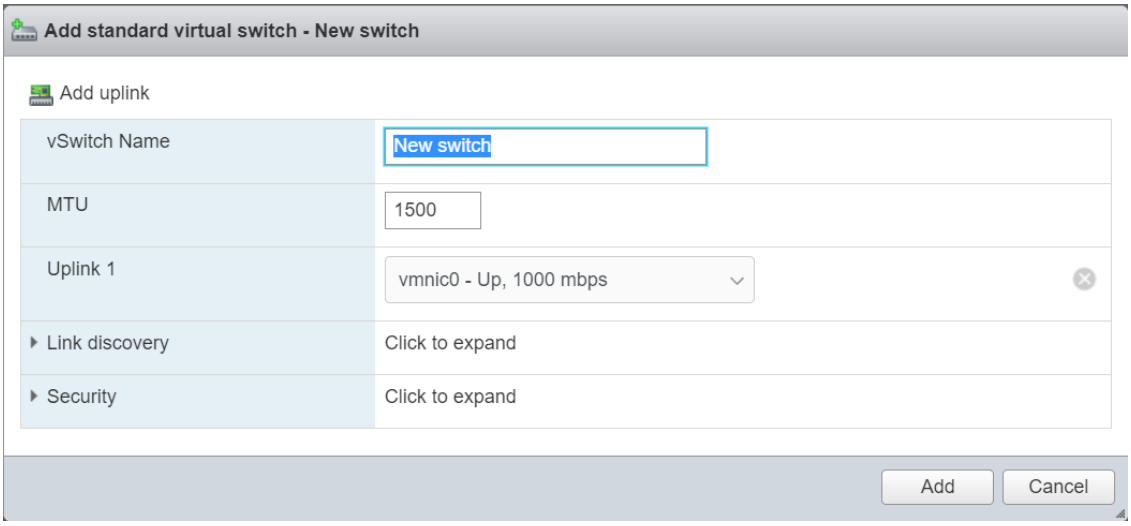
d. Click **Yes** to apply changes.



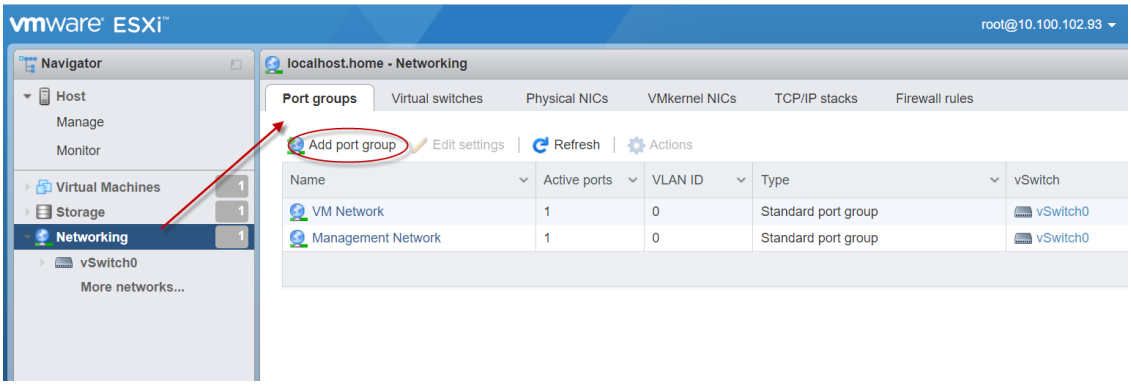
4. Press the Esc key, and then press the F12 key to restart the ZPLS.
5. Go to VMware management interface to continue the network related setup.
6. Select **Networking** from the left pane, select the **Virtual Switches** tab, and then the click **Add Standard virtual switch**:



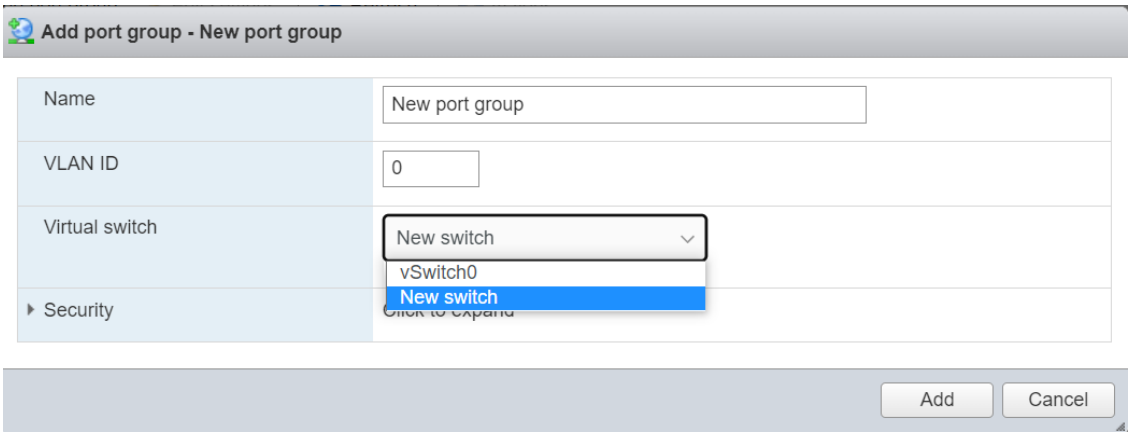
   a. Create the new vSwitch using the internal interface, vmnic0.



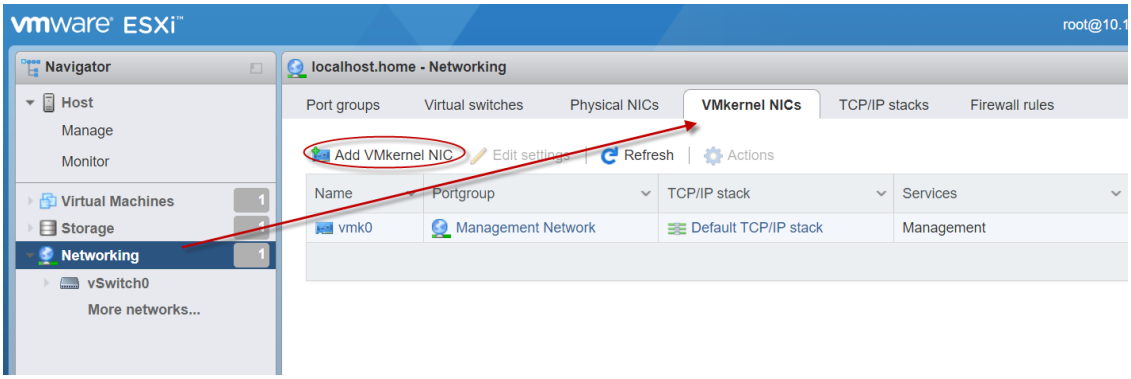
b. Select the **Add port group** tab, and then the click **Add port group**.



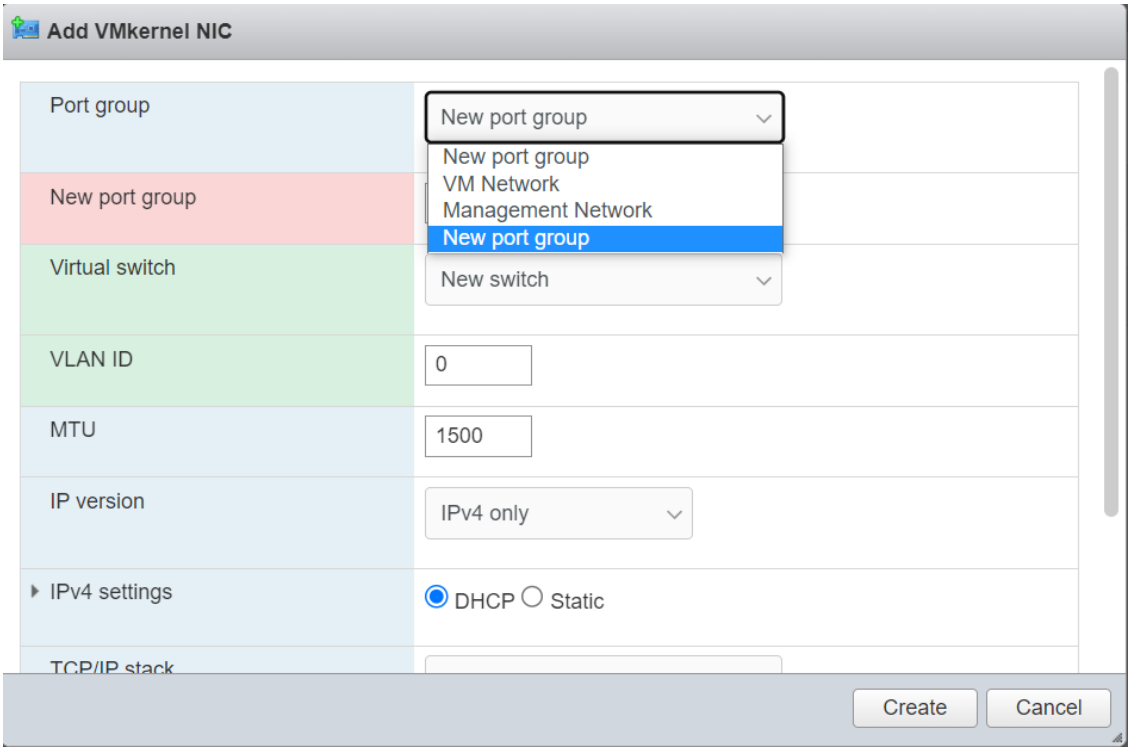
c. Select the newly created Virtual Switch.



d. Select the **VMkernel NICs** tab, and then the click **Add VMkernel NIC**.



e. Select the newly created Port group and click **Create**.



This page is intentionally left blank.

International Headquarters

1 Hayarden Street,

Airport City

Lod 7019900, Israel

Tel: +972-3-976-4000

Fax: +972-3-976-4040

AudioCodes Inc.

80 Kingsbridge Rd

Piscataway, NJ 08854, USA

Tel: +1-732-469-0880

Fax: +1-732-469-2298

Contact us: https://www.audiocodes.com/corporate/offices-worldwide

Website: https://www.audiocodes.com/

Documentation Feedback: https://online.audiocodes.com/documentation-feedback

Document #: LTRT-29401