CONFIGURATION GUIDE

RUCKUS Virtual Edge Getting Started Guide, 2.1.0

Supporting RUCKUS Edge 2.1.0 Release

Part Number: 800-73357-001 Rev A
Publication Date: October 2024

Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, COMMSCOPE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. CommScope does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. CommScope does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to CommScope that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

IN NO EVENT SHALL COMMSCOPE, COMMSCOPE AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF COMMSCOPE HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

CommScope and the CommScope logo are registered trademarks of CommScope and/or its affiliates in the U.S. and other countries. For additional trademark information see https://www.commscope.com/trademarks. All product names, trademarks, and registered trademarks are the property of their respective owners.

Patent Marking Notice

For applicable patents, see www.cs-pat.com.

Contents

Contact Information, Resources, and Conventions

Contacting RUCKUS Customer Services and Support

The Customer Services and Support (CSS) organization is available to provide assistance to customers with active warranties on their RUCKUS products, and to customers and partners with active support contracts.

For product support information and details on contacting the Support Team, go directly to the RUCKUS Support Portal using https://support.ruckuswireless.com, or go to https://www.ruckusnetworks.com and select **Support**.

What Support Do I Need?

Technical issues are usually described in terms of priority (or severity). To determine if you need to call and open a case or access the self-service resources, use the following criteria:

- Priority 1 (P1)—Critical. Network or service is down and business is impacted. No known workaround. Go to the **Submit a Case** section.
- Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the **Submit a Case** section.
- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Click the **CONTACT** tab at the top of the page and explore the **Self-Service Online Help** options.
- Priority 4 (P4)—Low. Requests for information, product documentation, or product enhancements. Click the **CONTACT** tab at the top of the page and explore the **Self-Service Online Help** options.

Open a Case

When your entire network is down (P1), or severely impacted (P2), call the appropriate telephone number listed below to get help:

- Continental United States: 1-855-782-5871
- Canada: 1-855-782-5871
- Europe, Middle East, Africa, Central and South America, and Asia Pacific, toll-free numbers are available at https://support.ruckuswireless.com/contact-us and Live Chat is also available.
- Worldwide toll number for our support organization. Phone charges will apply: +1-650-265-0903

We suggest that you keep a physical note of the appropriate support number in case you have an entire network outage.

Self-Service Resources

The RUCKUS Support Portal at https://support.ruckuswireless.com offers a number of tools to help you to research and resolve problems with your RUCKUS products, including:

- Technical Documentation—https://support.ruckuswireless.com/documents
- Community Forums—https://community.ruckuswireless.com
- Knowledge Base Articles—https://support.ruckuswireless.com/answers
- Software Downloads and Release Notes—https://support.ruckuswireless.com/#products_grid
- Security Bulletins—https://support.ruckuswireless.com/security

Using these resources will help you to resolve some issues, and will provide the Technical Assistance Center (TAC) with additional data from your troubleshooting analysis if you still require assistance through a support case or Return Merchandise Authorization (RMA). If you still require help, open and manage your case at https://support.ruckuswireless.com/case_management.

Document Feedback

RUCKUS is interested in improving its documentation and welcomes your comments and suggestions.

You can email your comments to RUCKUS at #Ruckus-Docs@commscope.com.

When contacting us, include the following information:

- Document title and release number
- Document part number (on the cover page)
- Page number (if appropriate)

For example:

- RUCKUS SmartZone Upgrade Guide, Release 5.0
- Part number: 800-71850-001 Rev A
- Page 7

RUCKUS Product Documentation Resources

Visit the RUCKUS website to locate related documentation for your product and additional RUCKUS resources.

Release Notes and other user documentation are available at https://support.ruckuswireless.com/documents. You can locate the documentation by product or perform a text search. Access to Release Notes requires an active support contract and a RUCKUS Support Portal user account. Other technical documentation content is available without logging in to the RUCKUS Support Portal.

White papers, data sheets, and other product documentation are available at https://www.ruckusnetworks.com.

Online Training Resources

To access a variety of online RUCKUS training modules, including free introductory courses to wireless networking essentials, site surveys, and products, visit the RUCKUS Training Portal at https://commscopeuniversity.myabsorb.com/. The registration is a two-step process described in this video. Create a CommScope account and then register for, and request access for, CommScope University.

Document Conventions

The following table lists the text conventions that are used throughout this guide.

TABLE 1 Text Conventions

Convention	Description	Example
`monospace`	Identifies command syntax examples	`device(config)# interface ethernet 1/1/6`
bold	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the **Start** menu, click **All Programs**.
italics	Publication titles	Refer to the *RUCKUS Small Cell Release Notes* for more information.

Notes, Cautions, and Safety Warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE
A NOTE provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An ATTENTION statement indicates some information that you must read before continuing with the current action or task.

CAUTION
A CAUTION statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER
A DANGER statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Command Syntax Conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{**x**| **y**| **z**}	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x|**y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a “soft” line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

About This Guide

Introduction

This *RUCKUS Virtual Edge Getting Started Guide* provides information on applications that are used to install and configure the RUCKUS Virtual Edge device. You can download the installation guide from RUCKUS support website:

https://support.ruckuswireless.com/documents

Before deploying RUCKUS Virtual Edge, refer to the latest software and the release documentation.

- Release Notes and other user documentation are available at: https://support.ruckuswireless.com/documents.
- Software upgrades are available at: https://support.ruckuswireless.com/software.
- Software license and limited warranty information are available at: https://support.ruckuswireless.com/warranty.

Introduction

Built to run on hardware as well as virtual platforms, RUCKUS Edge runs services as applications on hardware in the customer's local networks as well as independently if the switch connection is down.

Feature Overview

The RUCKUS Edge device is developed to provide distributed services to meet latency and fault tolerance requirements. The following are core principles in developing the RUCKUS Edge:

- The RUCKUS Edge device is developed using cloud-native design principles and interfaces.
- The infrastructure and application services are designed to run in any cloud-native compliant operating system.
- The RUCKUS Edge device's infrastructure and application services run in standard server hardware and on virtual machines.

Requirements

Ensure one of the following requirement is available to onboard a RUCKUS Edge device.

- VMware® ESXi™
- Linux® Kernel-based Virtual Machine (KVM)

Prerequisites

The following are the prerequisites to onboard a RUCKUS Edge device.

- A hypervisor on which to install RUCKUS Virtual Edge.
- A RUCKUS One account.
- A RUCKUS Edge virtual device (RUCKUS Virtual Edge) distribution package (.OVA file), available for download from the RUCKUS Support website.
- A Virtual Machine (VM) with recommended system resources for the number of APs and wireless clients to manage the network.
- For RUCKUS Edge to be managed by RUCKUS One, and to function properly, configure your firewall to allow for outbound connectivity according to the following guidelines.

  Outbound HTTPS (TCP 443) from RUCKUS Edge to:

  - https://ap-registrar.ruckuswireless.com
  - https://sw-registrar.ruckuswireless.com
  - https://ocsp.comodoca.com
  - https://ocsp.entrust.net
  - https://ruckus.cloud
  - https://eu.ruckus.cloud
  - https://asia.ruckus.cloud
  - https://device.ruckus.cloud
  - https://device.eu.ruckus.cloud
  - https://device.asia.ruckus.cloud

- https://storage.googleapis.com
- https://edge-docker-registry.asia.ruckus.cloud
- https://edge-docker-registry.eu.ruckus.cloud
- https://edge-docker-registry.ruckus.cloud

Installation Workflow

The RUCKUS Virtual Edge installation workflow is outlined in the following table.

TABLE 2 RUCKUS Virtual Edge Installation Workflow

Steps	Procedure	Description
Step 1	Installing and Starting RUCKUS Virtual Edge on the Hypervisor on page 15	This task comprises installing an instance of RUCKUS Virtual Edge on the hypervisor, configuring PCI devices, obtaining the device serial number, and configuring the RUCKUS Virtual Edge internal services network.
Step 2	Onboarding, Authentication and Authorization for RUCKUS One on page 41	This task comprises adding the RUCKUS Virtual Edge device to the RUCKUS One management platform and entering a one-time password to authenticate and onboard the RUCKUS Virtual Edge device, resulting in the device status changing to **Needs Configuration**.
Step 3	Configuring and Verifying RUCKUS Virtual Edge on RUCKUS One on page 53	This task comprises configuring port interfaces, a link aggregation group, a DNS server, and static routes for the RUCKUS Virtual Edge device, resulting in the device status changing to **Operational**.
Step 4	Configuring vSwitch on the ESXi Server for RUCKUS Edge on page 63	This task comprises configuring NTP to synchronize the time on the ESXi server with an external NTP server of your choosing, and enabling PCI passthrough on NIC ports to allow RUCKUS Virtual Edge device to directly access the server's physical GPU card, bypassing the hypervisor layer.
Step 5	Configuring vSwitch on the ESXi Server for RUCKUS Edge on page 63	This task comprises configurations on the ESXi server to add a standard virtual switch on the ESXi server (facilitating the RUCKUS Virtual Edge device connectivity with the network), add the vSwitch to a port group, and deploy the RUCKUS Virtual Edge device and port group.
Step 6	Configuring Dynamic Resource Allocation on page 69	This task allows you to modify the number of server hardware CPU resources available for dynamic allocation to the RUCKUS Virtual Edge services and applications.

Installing and Starting RUCKUS Virtual Edge on the Hypervisor

Installing and Starting RUCKUS Virtual Edge on the KVM

Preparing for Installation

KVM CPU/IO Requirements

TABLE 3 OS and Hardware Requirements

Component	Requirement
Supported OS versions	Debian 11, Rocky Linux 8
CPU	Intel i7 or higher with a minimum 2 physical CPU cores per instance
Memory	24 GB per instance
Disk	32 GB per instance
NICs	• 1Gbps: Intel I350 • 10Gbps: Intel X520, X550, X710, XL710, and X722
Optic Connectors	Intel-compatible
Core switch (for certain topologies)	RUCKUS ICX switch family or a third-party switch

Required Software Packages

Ensure the latest software packages are installed for upgrade and bug fixes.

TABLE 4 OS Versions

OS	Toolkit
Debian 11	libvirt-daemon-system, ovmf, qemu-system-x86, virtinst
Rocky Linux 8	libvirt, edk2-ovmf, qemu-kvm, virt-install

TABLE 5 Install Required Packages

OS	Command
Debian 11	`sudo apt-get update` `sudo apt-get install <PKG_NAME> [<PKG_NAME> ...]`
Rocky Linux 8	`sudo dnf update` `sudo dnf install <PKG_NAME> [<PKG_NAME> ...]`

libvirt

1. Check if **libvirtd** is running:

   ```
   pgrep libvirtd
   ```

   If nothing is returned by `pgrep`, start the libvirtd service manually:

   ```
   sudo systemctl start libvirtd.service
   ```

2. Make the **libvirtd** service automatically start at host boot:

   ```
   sudo systemctl enable libvirtd.service
   ```

3. Disable libvirtd AppArmor profile.

   TABLE 6 Disabling the Profile

OS	Command

Debian 11	By default, AppArmor is enabled for Debian 11.
	Unload **libvirtd** AppArmor profile.
	`sudo apparmor_parser -R /etc/apparmor.d/usr.sbin.libvirtd`
	`sudo ln -s /etc/apparmor.d/usr.sbin.libvirtd /etc/apparmor.d/disable/`

Rocky Linux 8	NA

Networking

vEdge needs at least one network interface to function, either a PCI passthrough or a virtio interface.

PCI Passthrough Support

Skip this section if there is no requirement to use NIC PCI passthrough.

1. Enable IOMMU support.

NOTE
You can check this by checking the status of the `/sys/kernel/iommu_groups` directory. If this directory exists and has content, IOMMU is likely enabled.

TABLE 7 Enabling IOMMU Support

Debian 11	Rocky Linux 8

Debian 11 Linux kernel has
`CONFIG_INTEL_IOMMU_DEFAULT_ON_INTGPU_OFF=y`
NOTE
No manual enabling required.
	If IOMMU is not enabled or you need to adjust its settings, you will usually need to modify your GRUB (or GRUB2) configuration, as follows: . Here's how you can do it:
	• Make a backup of the original **grub.cfg file.sudo grub2-mkconfig -o** *<GRUB_CFG_PATH>*
	NOTE
	The *<GRUB_CFG_PATH>* depends on the host OS installation type: legacy BIOS boot or UEFI boot. Find the original file grub.cfg in /boot and make a backup.
	• Edit the GRUB configuration file using a text editor (such as `nano` or `vi`):
	`sudo vi /etc/default/grub`
	• Locate the `GRUB_CMDLINE_LINUX` parameter and append `intel_iommu=on`.
	`GRUB_CMDLINE_LINUX="... intel_iommu=on"`
	• Save the file and exit the text editor.
	• After making changes to the GRUB configuration file, update GRUB to apply the changes.

2. Auto-insert the **vfio-pci** driver at boot.

```
echo 'vfio-pci' | sudo tee /etc/modules-load.d/vfio-pci.conf
```

3. Enable user access to the vfio device files.

NOTE
Ensure you log in using the user account that is going to execute the installation process and not the 'root' account.

For example, if the user *$USER* is the one that is going to execute the `.bin` file.

```
echo 'SUBSYSTEM=="vfio", OWNER="root", GROUP="kvm"' | sudo tee /etc/udev/rules.d/10-qemu-hw-
users.rules
sudo usermod -aG kvm "$USER"
```

4. Edit `/etc/security/limits.conf`, for example, `sudo vi /etc/security/limits.conf` and add the two lines for the normal user that is going to execute the `.bin` file to unlimit memlock.

```
foo soft memlock unlimited
foo hard memlock unlimited
```

NOTE
Replace *foo* with your account name (not the root) that is going to execute the installation process.

5. Reboot the host after completing the preparation for PCI passthrough and verify:
   - If IOMMU is enabled by checking the `/sys/kernel/iommu_groups` directory again.
   - If vfio-pci is loaded by entering the: `lsmod | grep vfio_pci` command again.

Virtual Network

1. Skip this section if there is no requirement to use virtio virtual network interfaces.

   Use one of the following methods to create bridges for vEdge.

   - Using libvirt commands and XML-based configurations.

     TABLE 8 Example: libvirt default network

Debian 11	Rocky Linux 8

`sudo virsh net-define /etc/libvirt/qemu/networks/default.xml`
`sudo virsh net-start default`
`sudo virsh net-autostart default`
 	
A bridge, `virbr0`, with NAT/DHCP services is created and is ready for virtio interfaces to attach.
	The configuration is enabled by default when `libvirt` is installed and started.
	A bridge, `virbr0`, with NAT/DHCP services is created and ready for virtio interfaces to attach.

   - Manually create a bridge using the following commands:

     ```
     sudo ip link add name vse-br0 type bridge
     sudo ip link set dev vse-br0 up
     ```

     Add some host network interfaces, for example, eth0 to the bridge

     ```
     sudo ip link set dev eth0 master vse-br0
     ```

     Add NAT/DHCP services for devices that connect to the bridge.

     A bridge named **vse-br0** is created and ready for virtio interfaces to attach.

2. Enable permission to access bridges.

   This applies to both methods listed in the previous step.

   TABLE 9 Permission to Access Bridges

Debian 11	Rocky Linux 8
`sudo mkdir -p /etc/qemu` `sudo vi /etc/qemu/bridge.conf`	`sudo vi /etc/qemu-kvm/bridge.conf`

3. Provide permission to create network tunnel devices.

   TABLE 10 Permission to Create Network Tunnel Devices

Debian 11	Rocky Linux 8
`sudo chmodu+s /usr/lib/qemu/qemu-bridge-helper`	By default, `/usr/libexec/qemu-bridge-helper` has already been set with `setuid`.

Installing the vEdge on a Kernel-based Virtual Machine Hypervisor

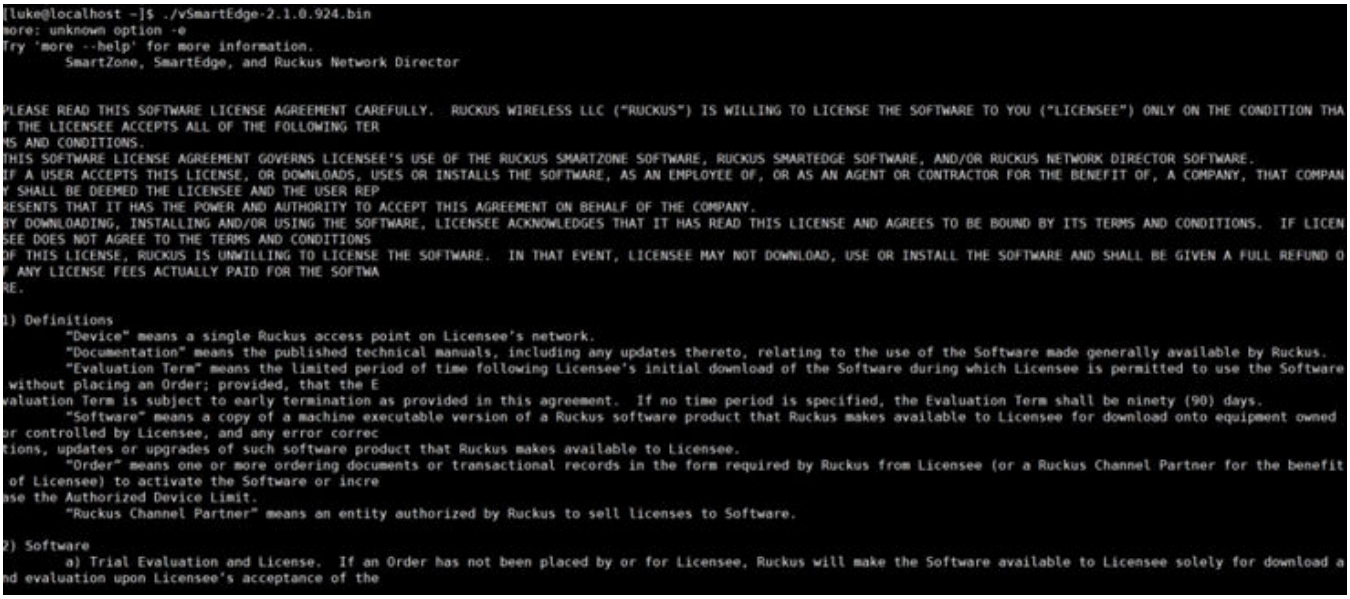
This section describes how to install the vEdge on a KVM hypervisor.

1. Download the `vSmartEdge-2.1.0.xxx.bin` file that includes the QCOW2 and tool script.
2. Copy the image to the KVM.
3. Open the terminal window.

4. Make the image bin file executable by entering the following command: **./vSmartEdge-2.1.0.924.bin**. For example: use *2.1.0.924* version.

   The End User License Agreement (EULA) is displayed.

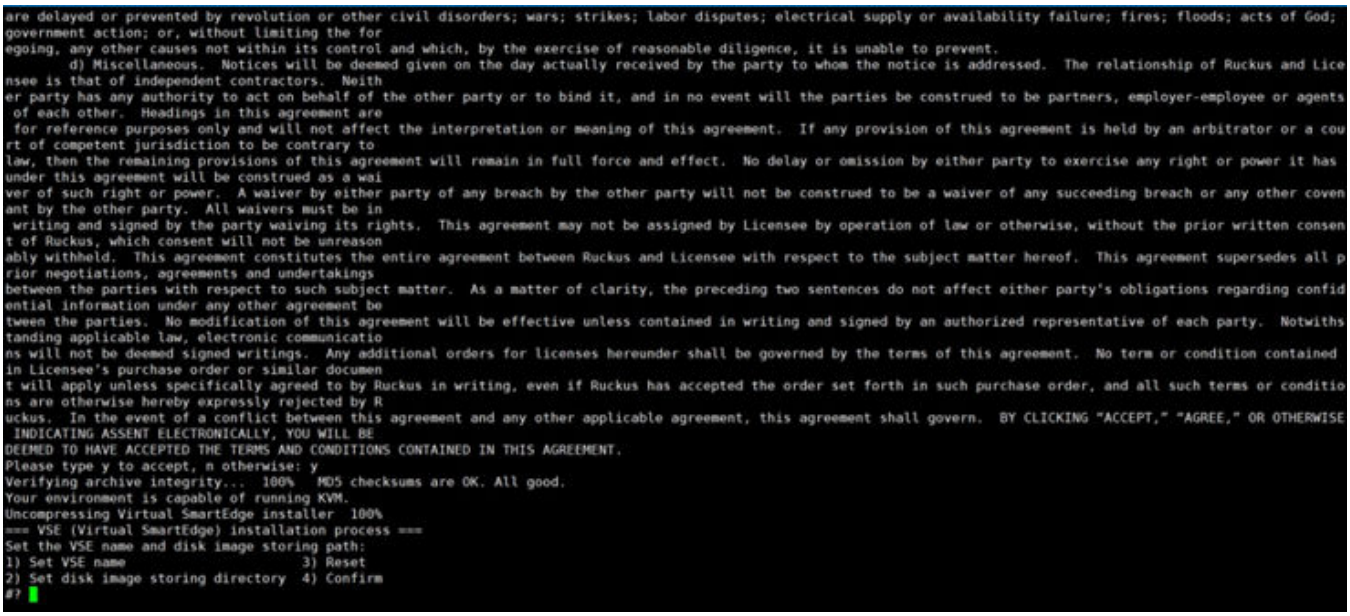
   FIGURE 1 RUCKUS Virtual Edge End User License Agreement



5. After checking the EULA, enter **y** to accept the agreement.

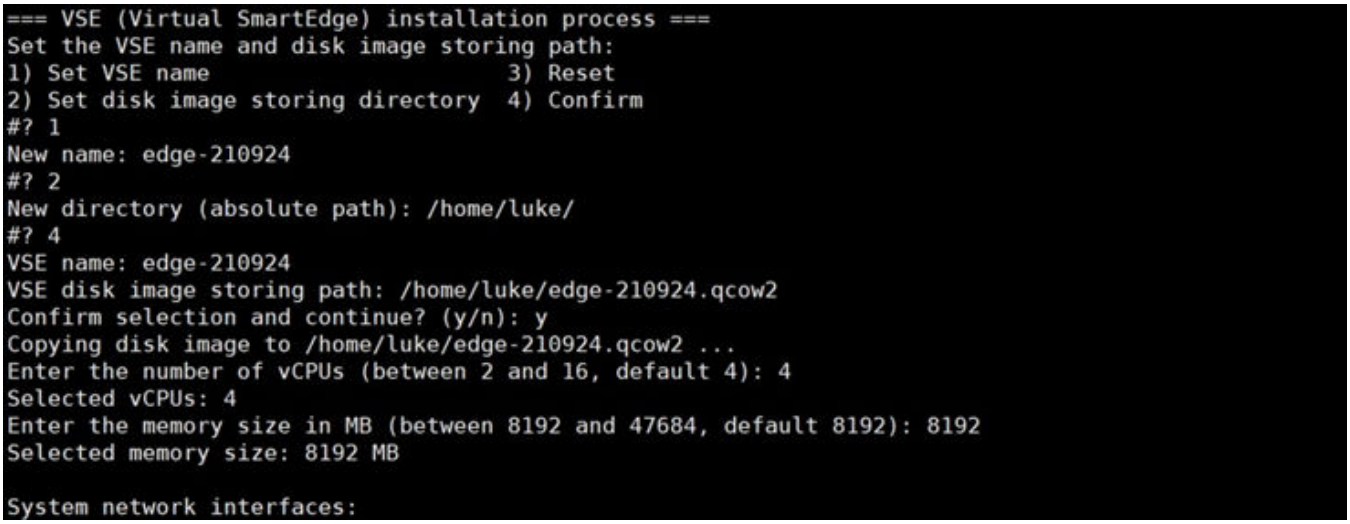
   The Virtual Edge installation process begins.

   FIGURE 2 Virtual Edge Installation Process



6. In the new vEdge, configure the following:
   - Enter **1** and enter a **New name** for the vEdge.
   - Enter **2** and enter the **New directory (absolute path)**. The location where you want to store the vEdge disk image.
   - Enter **4** to confirm the name and directory for the new vEdge device.
7. Enter **Y** to confirm select and continue.
8. Configure the number virtual CPUs and memory size required for the vEdge VM host.
   - **Selected vCPUs**
   - **Selected memory size**

   FIGURE 3 Configuring vCPUs and Memory Size

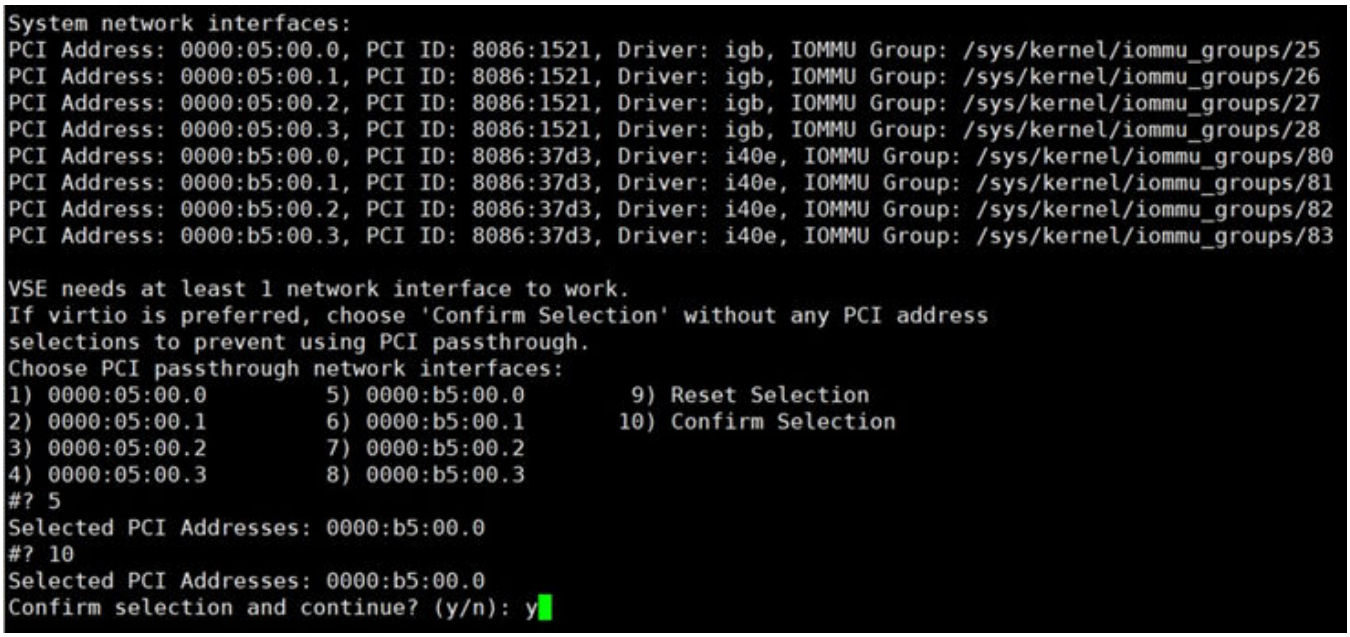


9. (Optional) You must configure at least one network interface for vEdge to operate. The interface can either be a PCI or a virtio interface, or a combination of both. To configure a PCI interface, enter the PCI ID corresponding to the selected PCI passthrough interface.

   The address of the selected PCI interface is displayed.
10. Enter **10** to confirm the selection.

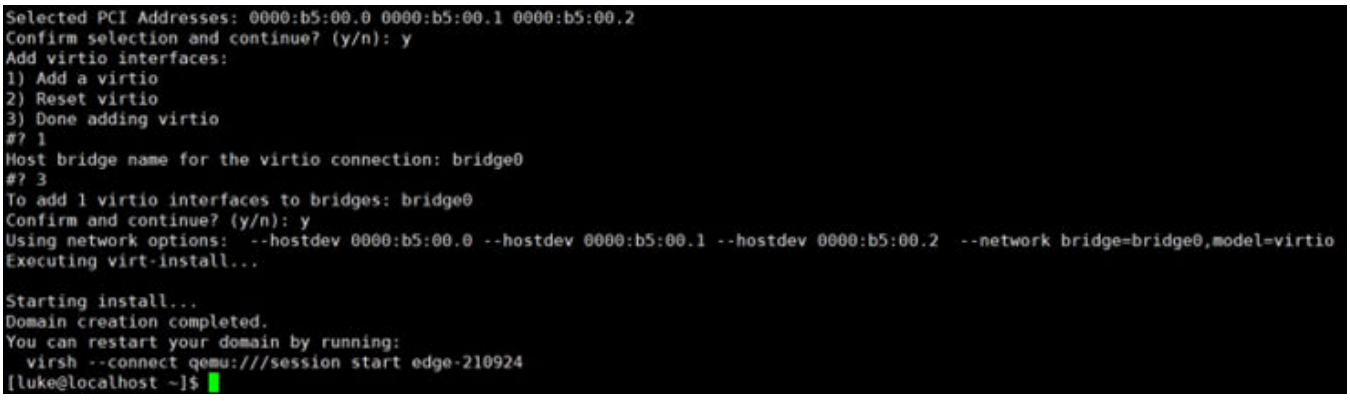
11. Enter **y** to **Confirm selection and continue**.

FIGURE 4 Configuring PCI Interface



12. (Optional) If you choose to add a virtio interface, type **1** and press enter. Else, proceed to Step 14.
13. At the **Host bridge name for the virtio connection** prompt, type the bridge name and press enter.
14. Type **3** and press enter.
15. At the **Confirm and continue?** prompt, type y and press enter.

FIGURE 5 Virtio Interface Selection

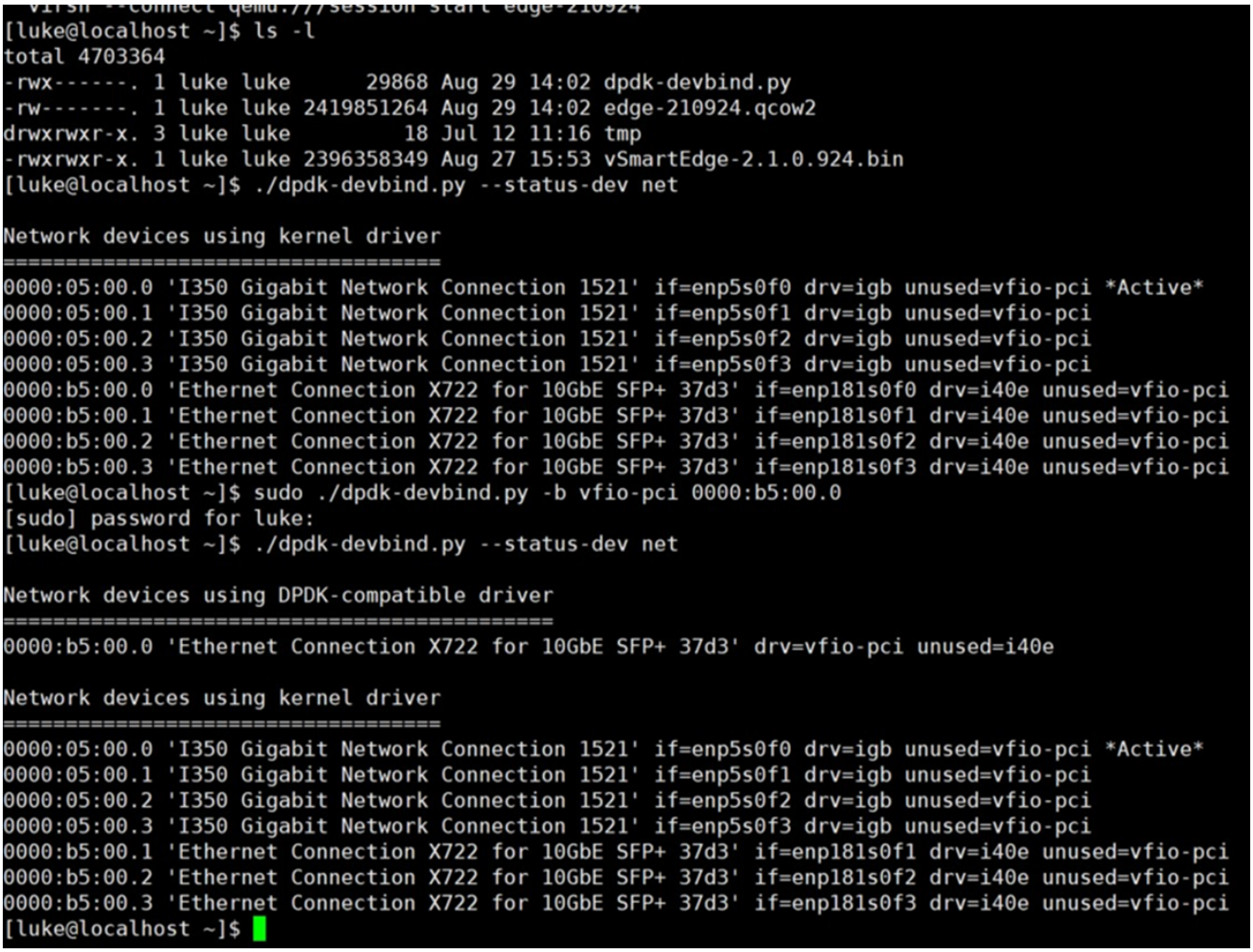


16. (Optional) Rebind network device drivers. Enter **./dpdk-devbind.py --status-dev net** to view the status of the PCI passthrough devices.

NOTE
Skip Step 16 and Step 17 if no PCI passthrough interface was selected in Step 9.

17. Enter **sudo ./dpdk-devbind.py -b vfio-pci** *<PCI device ID>* to rebind the selected PCI passthrough device to the vfio-pci usage.

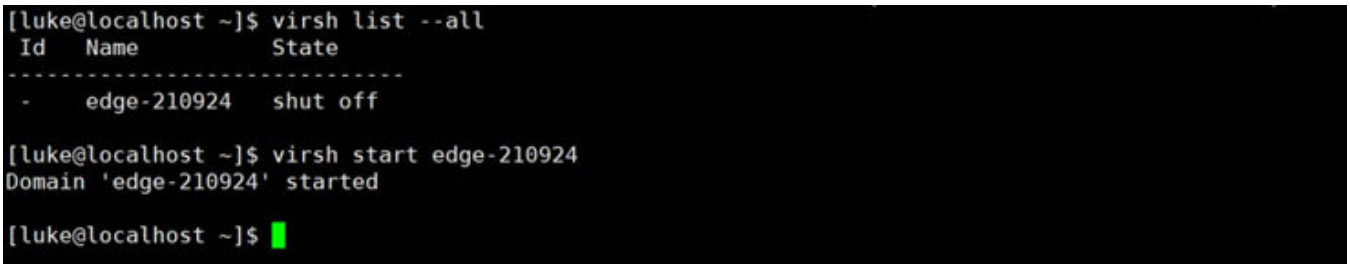
FIGURE 6 Rebinding the PCI Passthrough Device



After the vEdge script is deployed, by default, the Edge VM is powered off.

18. Manually power on the virtual machine using the command: **virsh start** [*<VSE_NAME>*].

FIGURE 7 Virtulal Edge Setup on KVM



You have completed setting up virtual Edge on the KVM hypervisor.

Installing and Starting RUCKUS Virtual Edge on EXSi

Preparing for Installation

VMware® ESXi™ Requirements

TABLE 11 System Requirements

Hardware and Software	System/Version
VMWare	VMware® ESXi™ 6.7, 7.0, or later
CPU	Intel i7 or higher with 4 physical CPU cores per instance
Memory	• 8 GB per instance
Disk Requirements	32 GB per instance
NIC Cards	10Gbps: Intel I350, X520, X520, X550, X710, XL710, and X722
Optic Connectors	Intel-compatible
Core switch (for certain topologies)	RUCKUS ICX switch family

Installing and Starting RUCKUS Virtual Edge on EXSi

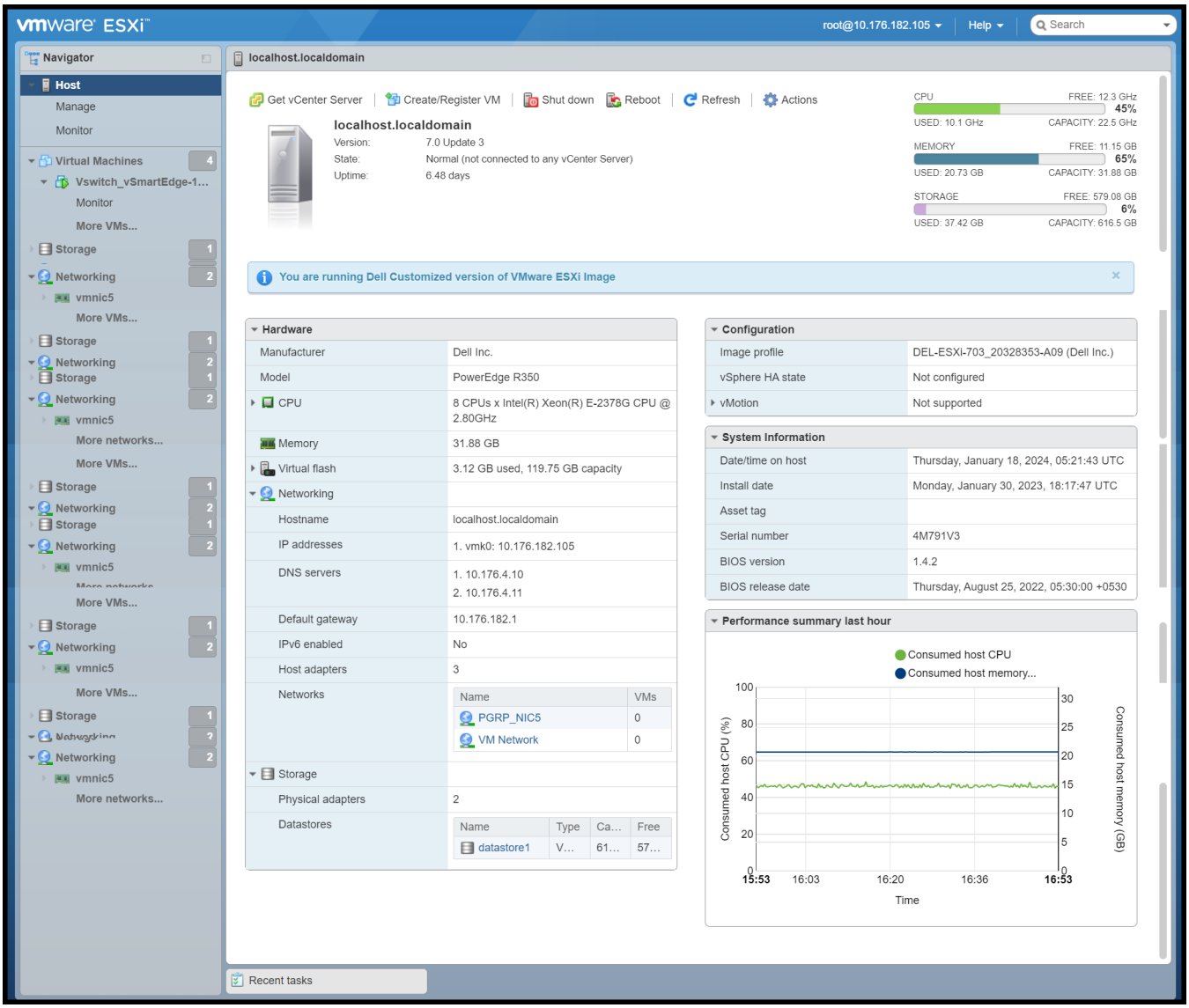
To deploy RUCKUS Virtual Edge on the physical server, ensure to connect the WAN cable and the optional LAN cable to the appropriate physical ports on the Network Interface Card (NIC).

Use the .OVA file downloaded from the RUCKUS Support site and install an instance of RUCKUS Virtual Edge on the hypervisor.

1. Log in to VMware® ESXi™.

   This displays the **VMware® ESXi™** home page.

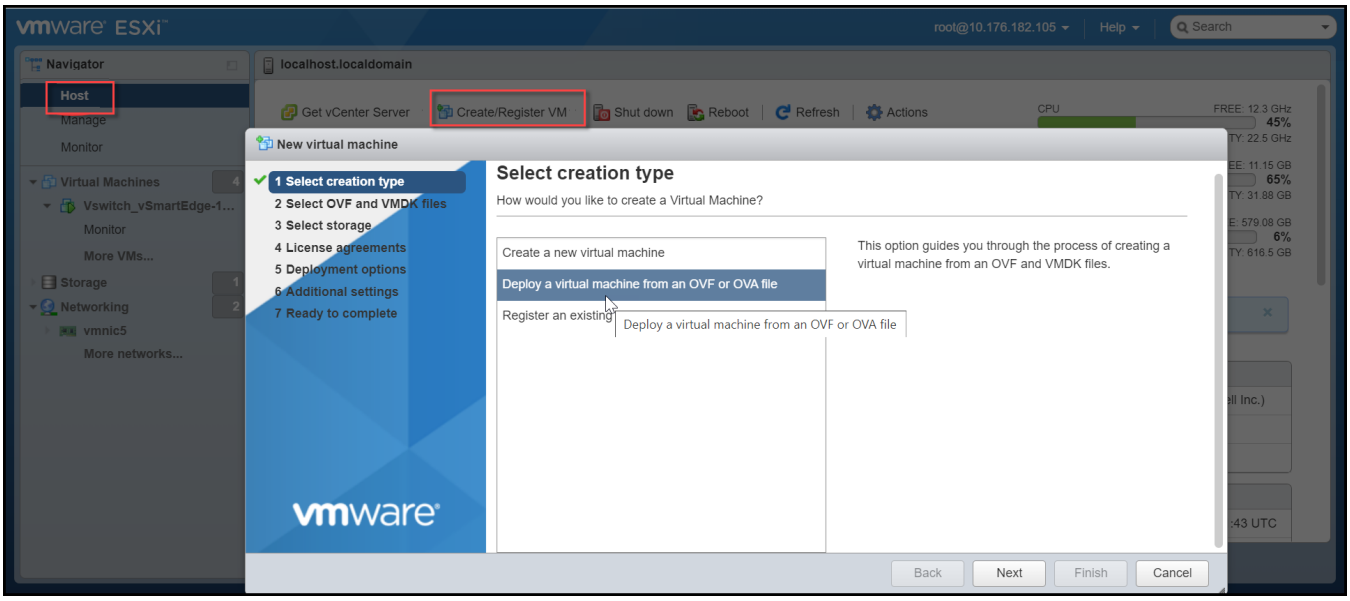
   FIGURE 8 VMware® ESXi™ Screen



2. Click **Host** > **Create/Register VM**.

   This displays the **New virtual machine** window. In this window, click **Deploy a virtual machine from an OVF or OVA file** and click **Next**. This displays the **Select OVF and VMDK files** screen.

   FIGURE 9 Select a Creation Type

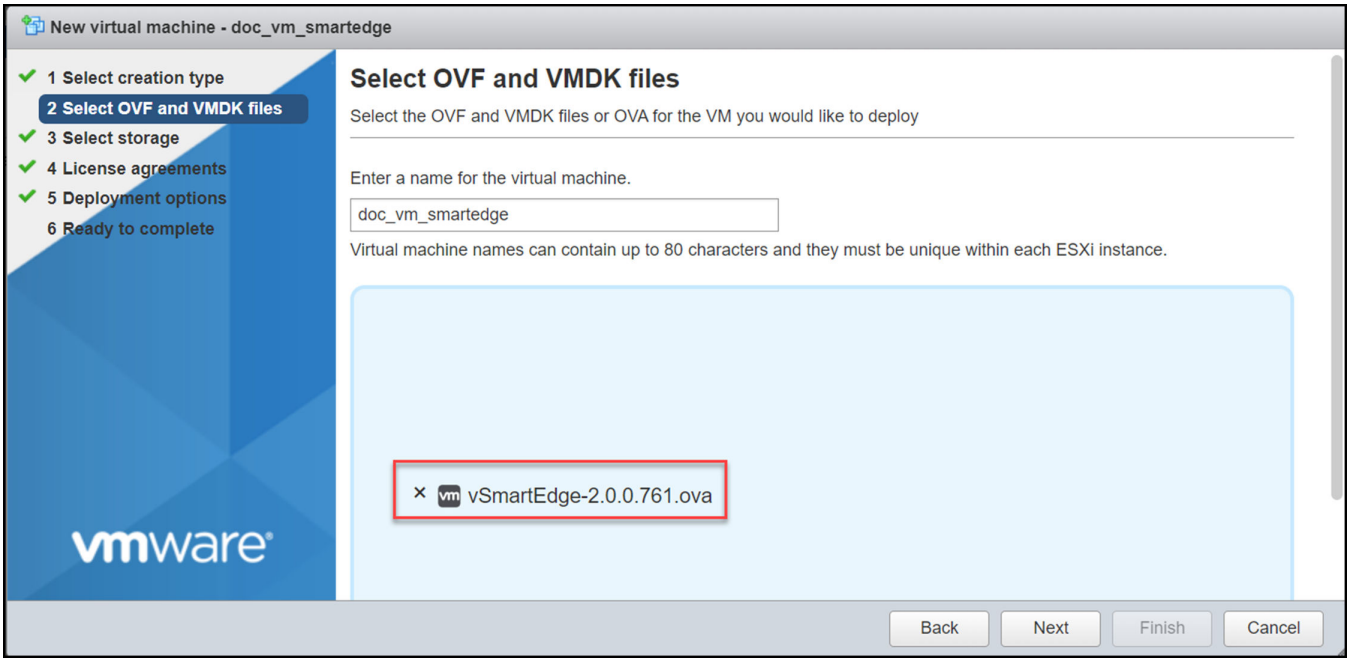


3. In the **Select OVF and VMDK files** screen, enter a name for your virtual machine.

4. Select the RUCKUS Virtual Edge .OVA file that you downloaded from the RUCKUS Support website and click **Next**.

   This displays the **Select storage** screen.

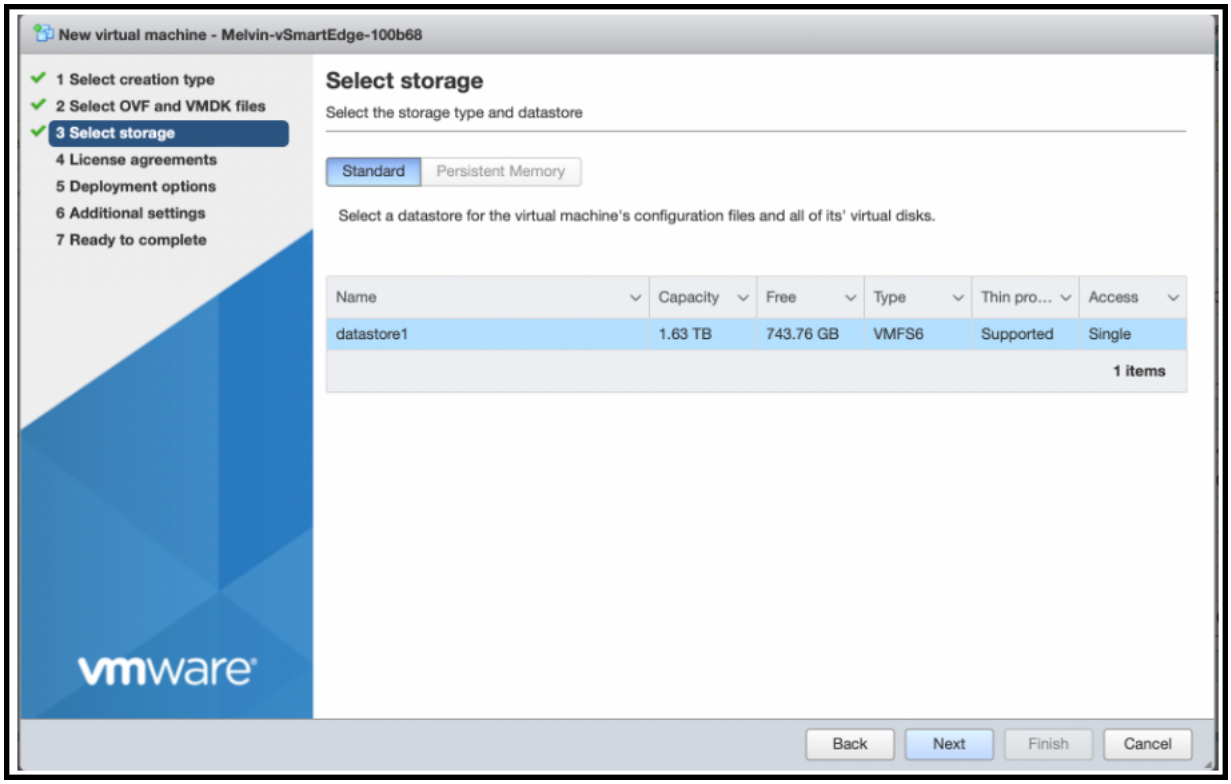
FIGURE 10 Select OVF and VMDK Files - Select OVA File



5. In the **Select storage** screen, select the datastore for the virtual machine and click **Next**.

   This displays the end-user license agreement screen.

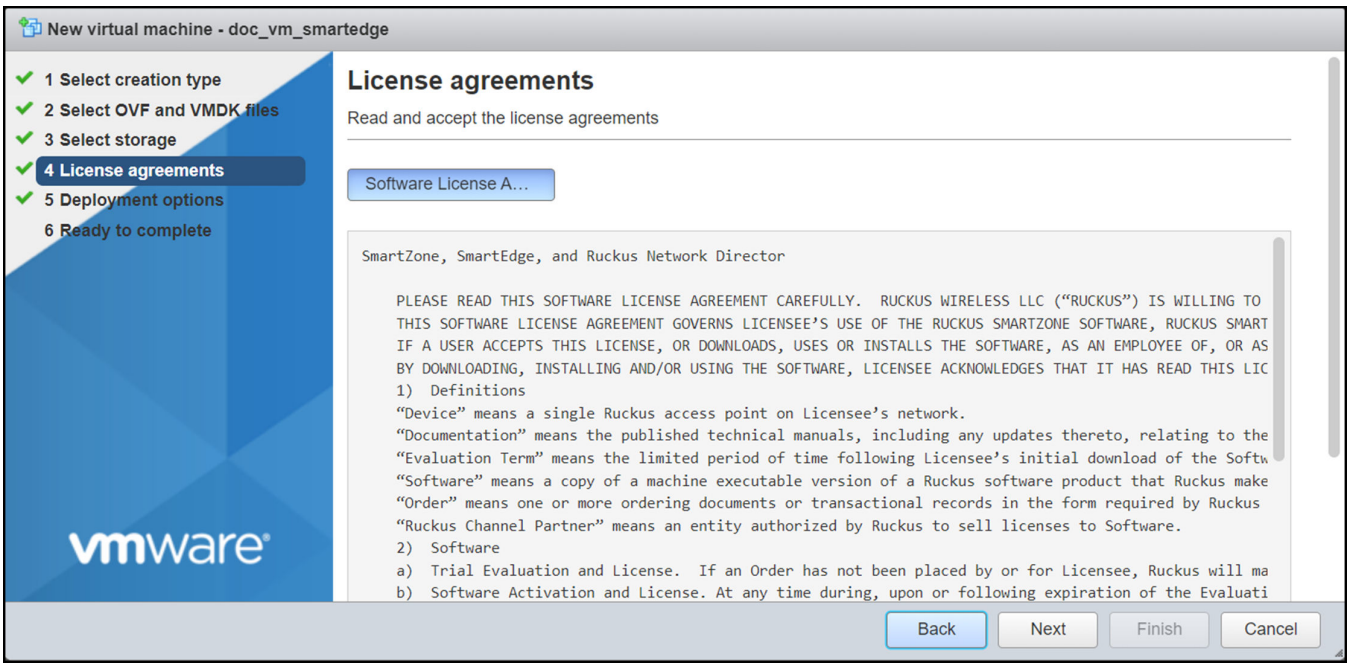
FIGURE 11 Select Storage



6. Read and accept the end-user license agreement on the **License agreements** screen, then click **Next**.

   This displays the **Deployment options** screen.

FIGURE 12 License Agreement

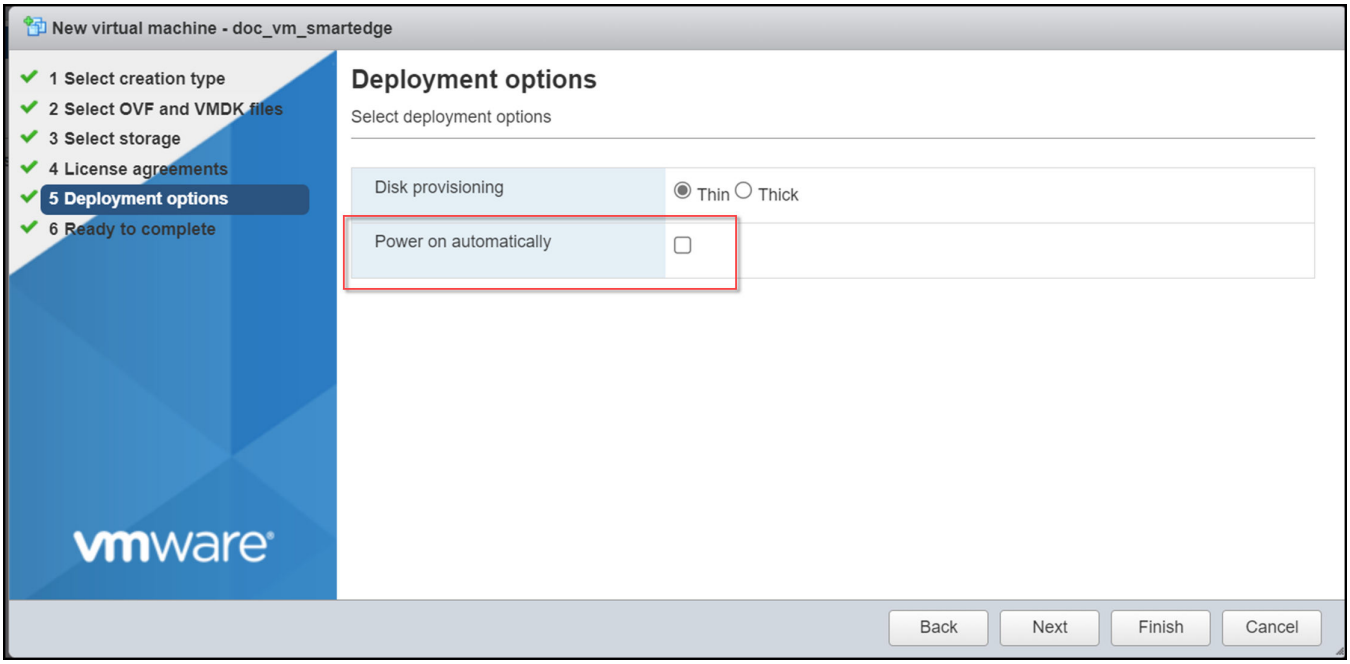


7. For the **Disk provisioning** option, select **Thin** or **Thick**.
   - **Thin**: Use this format to save storage space. For the thin disk, you provision as much datastore space as the disk would require based on the value that you enter for the virtual disk size.
   - **Thick**: A type of thick virtual disk that supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time.

   Clear the **Power on automatically** checkbox and click **Next**.

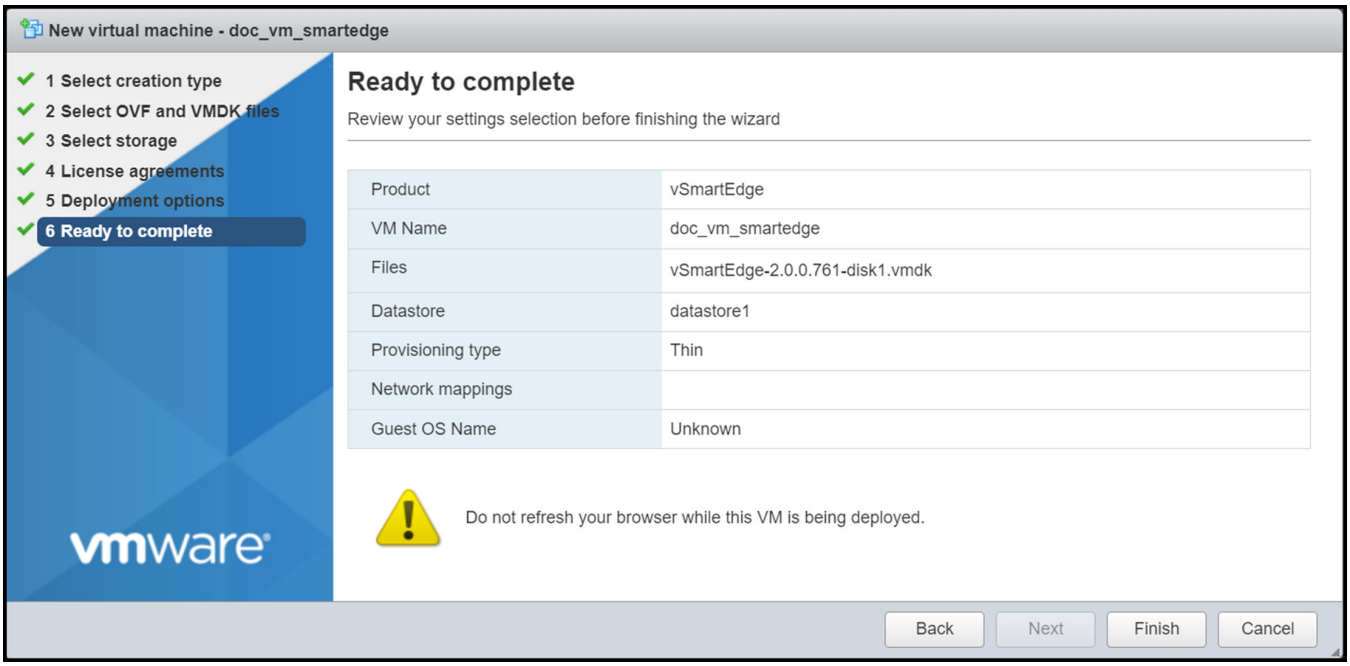
   This displays **Ready to Complete** screen.

FIGURE 13 Deployment Options



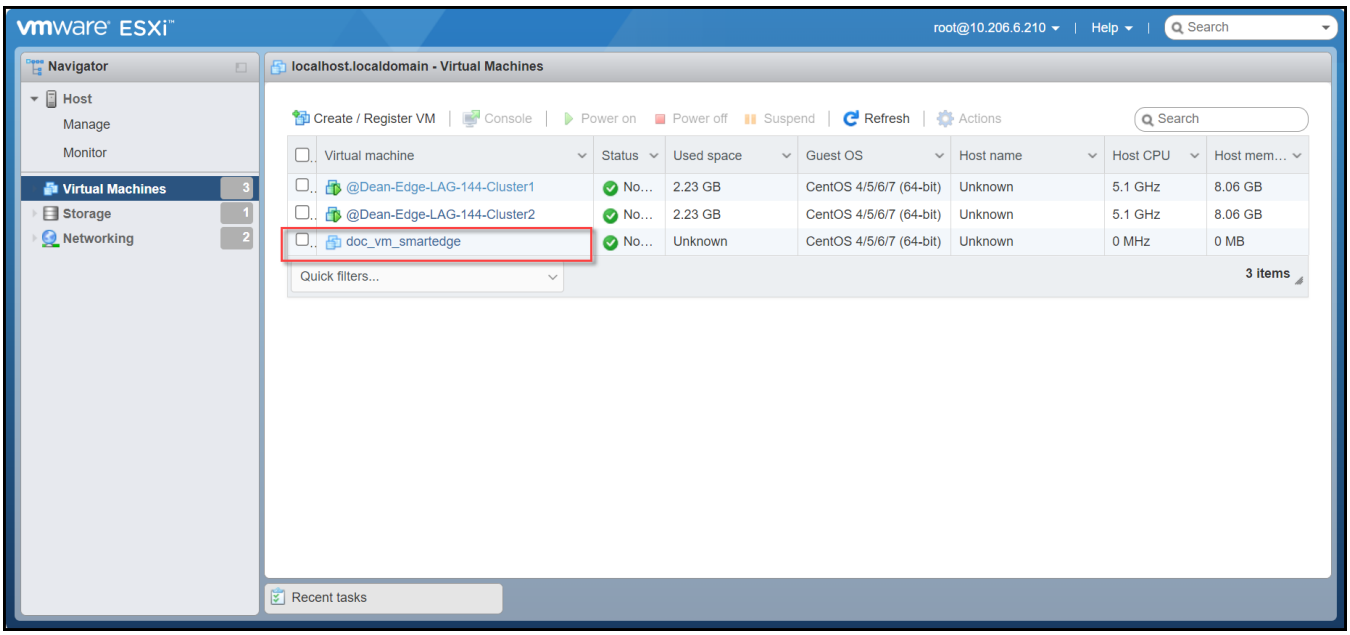
8. In the **Ready to Complete** screen, verify the details and click **Finish**. The new virtual machine is set up.

FIGURE 14 Ready to Complete



9. You can view the newly deployed RUCKUS Virtual Edge machine in the home page.

FIGURE 15 Newly Added Virtual Machine in the Home Page

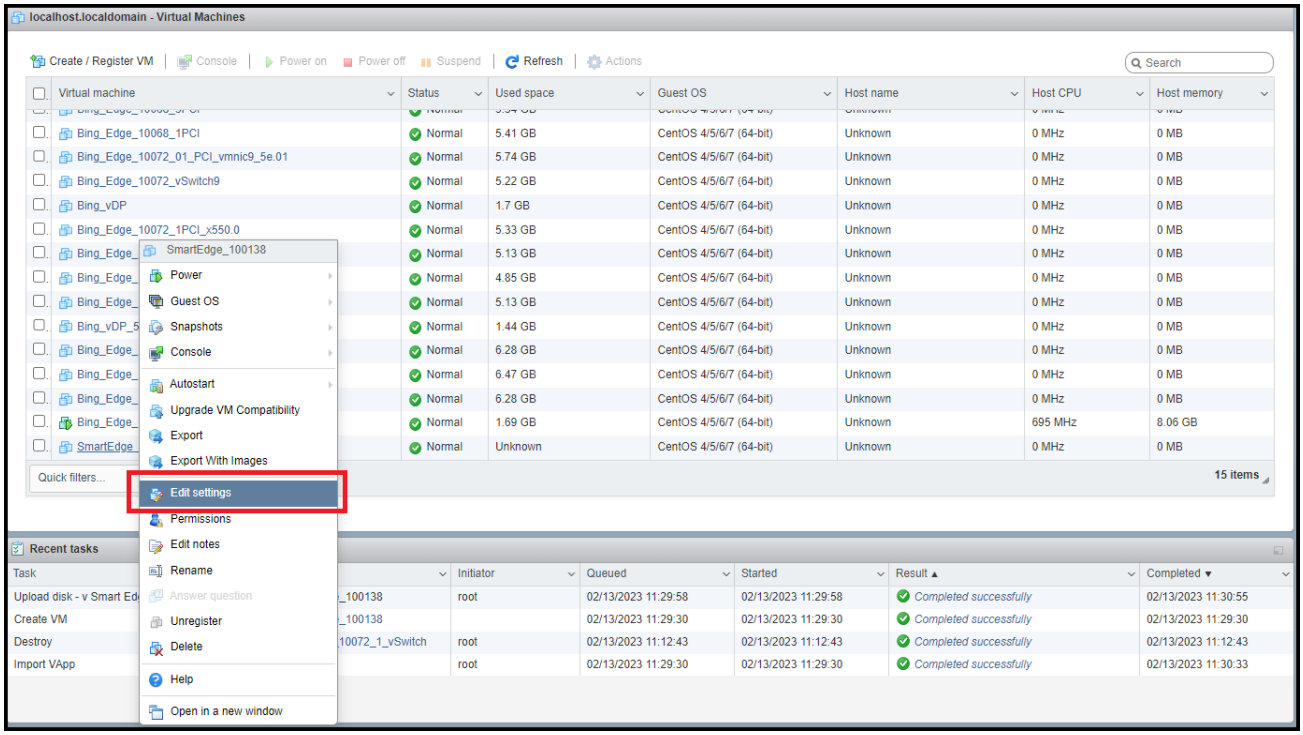


10. After setting up the new virtual machine, configure Peripheral Component Interconnect (PCI) passthrough interfaces for RUCKUS Virtual Edge.

    To configure PCI passthrough, perform the following:

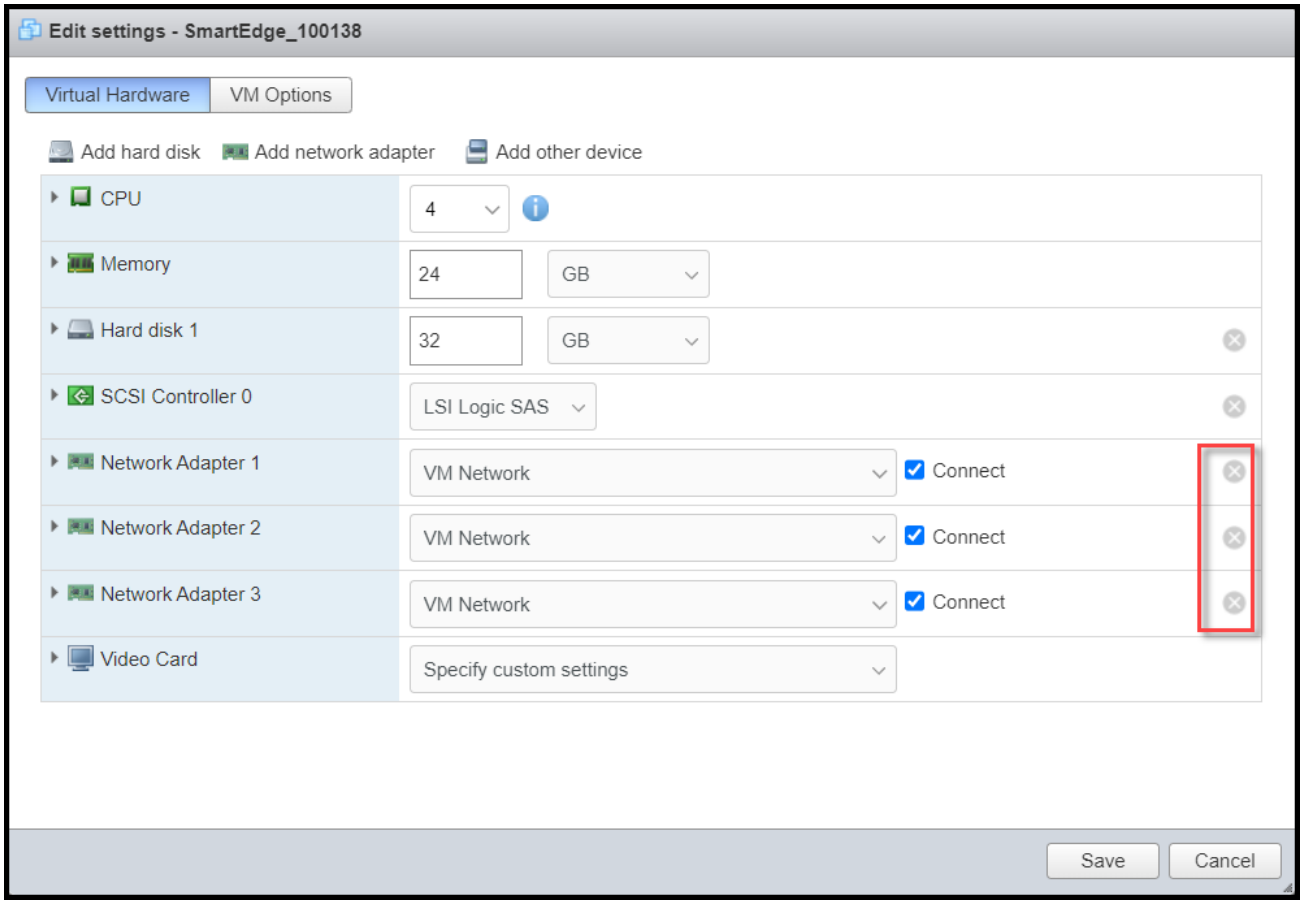
    a. Select the virtual machine from the list and right-click and then click **Edit settings**. This displays the **Edit Settings** window.

    FIGURE 16 Edit Settings



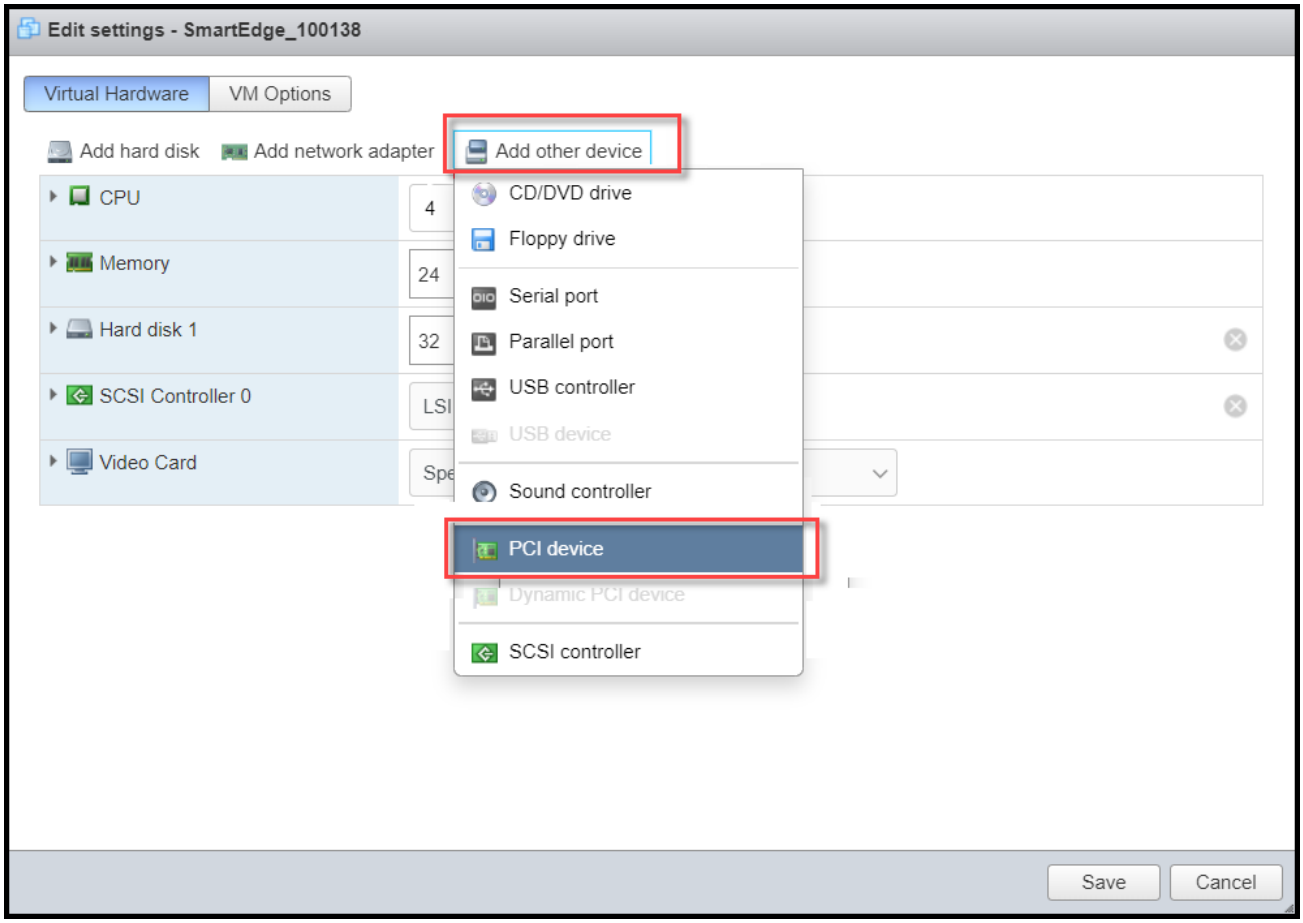
    b. In the **Edit Settings** window, remove all the network adapters from the RUCKUS Virtual Edge.

FIGURE 17 Virtual Network Interfaces



c. Click **Add other device** and select **PCI device** to add PCI passthrough interfaces for RUCKUS Virtual Edge.

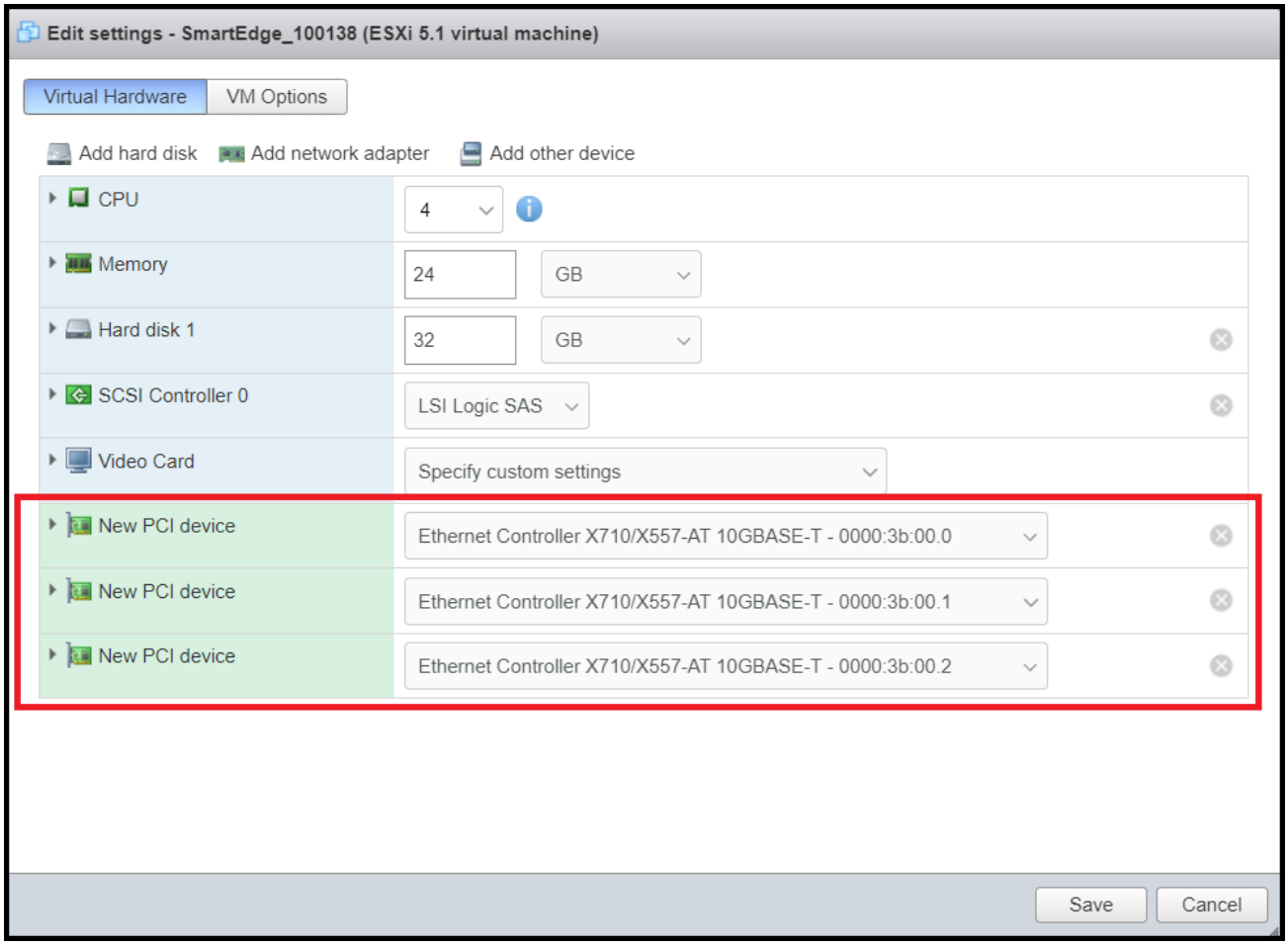
FIGURE 18 Adding PCI Passthrough Device



d. Review and confirm the PCI passthrough interfaces and click **Save**. The settings are saved.

NOTE
The RUCKUS Virtual Edge device minimally requires one PCI passthrough interface, but supports up to three.

FIGURE 19 PCI Passthrough Devices Added



Obtaining the RUCKUS Virtual Edge Serial Number and Interface IP Addresses

After successfully deploying and powering on the RUCKUS Virtual Edge, you can obtain the serial number, as well as view and manage the interface IP addresses, for your vEdge by using the command line interface (CLI) on the hypervisor.

Refer to the *RUCKUS Edge Command Reference Guide* for syntax and usage of commands used for configuring and managing the Edge devices.

To access the CLI and use the applicable commands, perform the following on the hypervisor interface:

1. Right-click on the RUCKUS Virtual Edge name and click **Console**.

   You can open the console in a new window.

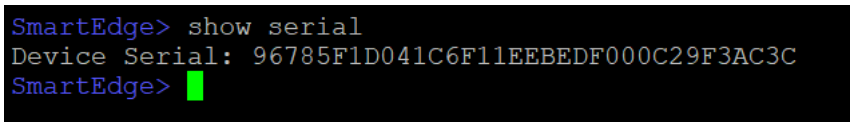
2. Log in to the console using the credentials: **Username**: admin, **Password**: admin.

   This displays the device serial number, QR code, and other device information.

   FIGURE 20 Serial Number and QR Code

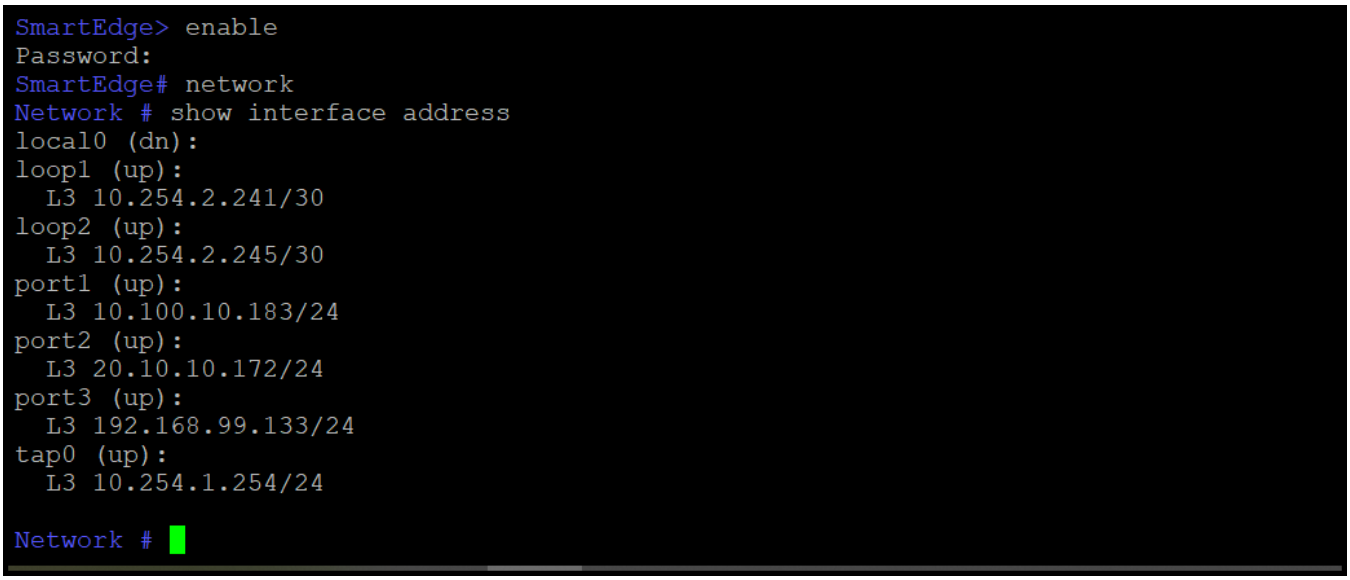
3. Although the serial number is displayed at log-on, at any time you may display the vEdge device serial number by entering the **show serial** command.

   FIGURE 21 Using the show serial Command



4. To view the interface IP addresses for your vEdge, enter network mode, using the **enable** command followed by the **network** command. In network mode, enter the **show interface address** command. The IP addresses listed under port1, port2, and port3 correspond to the interface IP addresses.

   FIGURE 22 Using the show interface address Command



   To configure static IP address, enter network mode, then enter the **set interface ip address** command, as shown in the example below:

```
SmartEdge> enable
Password:
SmartEdge# network
Network # set interface ip address port1 192.168.1.1/24 192.168.1.254
```

   To delete static IP address, enter network mode, then enter the **set interface ip address** command using **del** the option, as shown in the example below:

```
SmartEdge> enable
Password:
SmartEdge# network
Network # set interface ip address del port1 192.168.1.1/24 192.168.1.254
```

Internal Services Network

The RUCKUS Virtual Edge device, by default uses the network address and mask `10.254.0.0/16` for internal services.

If the RUCKUS Virtual Edge environment is deployed on the same network, it causes redundancy. To avoid such conflicts, RUCKUS Virtual Edge provides a command line interface that allows the user to change the IP address of the internal services network.

ATTENTION

The command **set internal-network** should be used *before* enrolling the RUCKUS Virtual Edge device with Ruckus One. If the device is already enrolled with RUCKUS One, executing this command is rejected to prevent configuration and data loss.

It is recommended to execute the command **set internal-network** from the console. If the system is rebooting, then the network is terminated.

If the internal network has to be changed after the device is enrolled with RUCKUS One, you should first delete the device from RUCKUS One. This restores the device to the deployment state, allowing you to change the internal network using the command **set internal-network**.

To change the internal network address, perform the following:

1. Enter the **show internal-network** command to view the internal network IP address. By default, the RUCKUS vEdge uses `10.254.0.0/16` for the internal services.

FIGURE 23 show internal-network

2. Enter the **set internal-network <ipv4-address>** to change the internal services network, if the RUCKUS Virtual Edge environment is deployed on the same network. When prompted to confirm the operation, type **yes**. The vEdge device will reboot.

FIGURE 24 set internal-network Command

NOTE
The **set internal-network** command in RUCKUS Virtual Edge automatically adds the required network prefix (**16**) for internal services.

3. After the reboot, log in with your credentials into the console and enter the command **show internal-network** to check settings.

FIGURE 25 New Internal Network Enabled

Onboarding, Authentication and Authorization for RUCKUS One

RUCKUS One is used to manage your RUCKUS Virtual Edge device. Onboarding a RUCKUS Virtual Edge device with RUCKUS One is a two-step process:

1. Add the RUCKUS Virtual Edge to RUCKUS One as per your platform preference:
   - RUCKUS One web interface - Refer to Adding a RUCKUS Edge through the Web User Interface on page 41 for detailed instructions.
   - RUCKUS One mobile application - Refer to Adding RUCKUS Edge through the Mobile Application on page 44 for detailed instructions.
2. Authorize and authenticate the RUCKUS Virtual Edge device using a one-time password - Refer to Authenticating the RUCKUS Virtual Edge Using the OTP on page 50 for detailed instructions.

Adding a RUCKUS Edge through the Web User Interface

The RUCKUS Edge device must already be successfully installed and deployed on the hypervisor. Refer to Installing and Starting RUCKUS Virtual Edge on the Hypervisor on page 15 for detailed instructions.

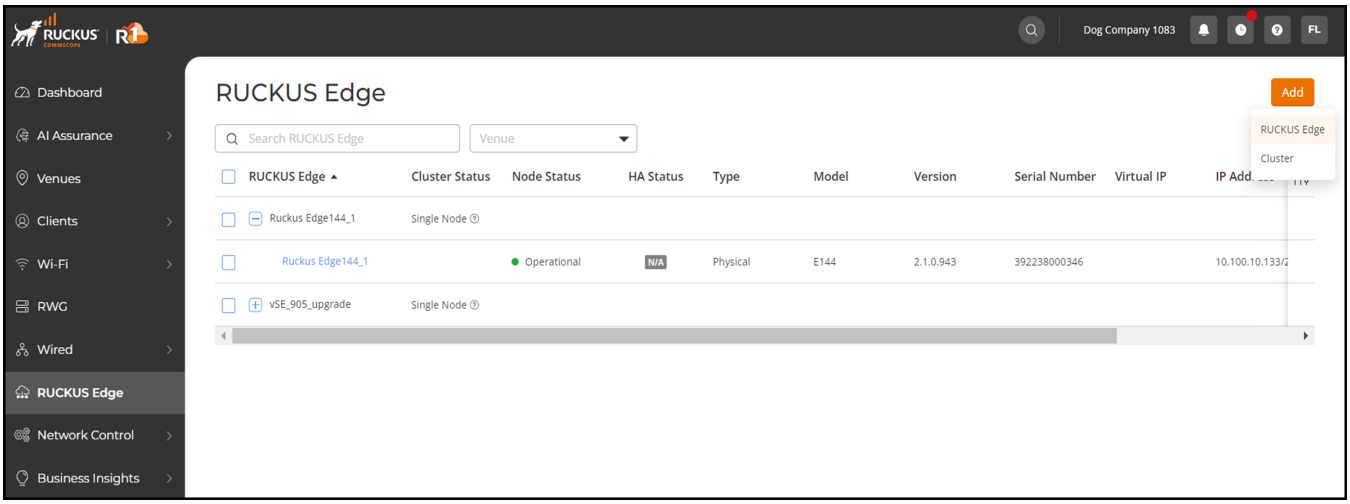
To add a RUCKUS Edge via the RUCKUS One web interface, perform the following:

1. Log in to the RUCKUS One web user interface with your RUCKUS One credentials.
2. In the **RUCKUS One** menu, click **RUCKUS Edge**.

   This displays the **RUCKUS Edge** page.

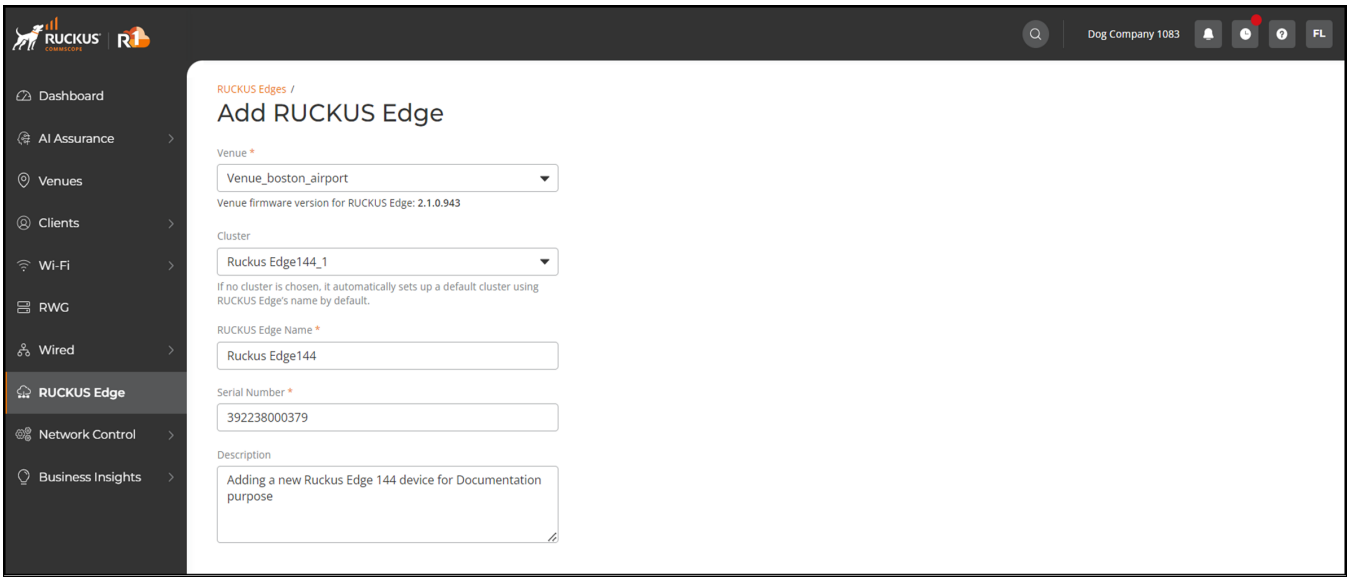
3. In the **RUCKUS Edge** page, click **Add** and select **RUCKUS Edge**. This displays the **Add RUCKUS Edge** page.

FIGURE 26 Add RUCKUS Edge



4. In the **Add RUCKUS Edge** page, enter the following details:
   - **Venue**: Click the drop-down arrow to select a site to associate with the RRUCKUS Edge device. A venue represents a physical space where networking devices are deployed.
   - **Cluster**: (Optional) Click the drop-down arrow to select the cluster to associate with RUCKUS Edge device. Set this field only if you are adding multiple RUCKUS Edge devices for redundancy. A cluster is a group of nodes which act as a single system to provide high availability and load balancing.
   - **RUCKUS Edge Name**: Enter a meaningful name for the RUCKUS Edge device.
   - **Serial Number**: Enter the serial number of the RUCKUS Edge device. The serial number can be viewed either by entering the command **show serial** or scanning the **QR** code; refer to Obtaining the RUCKUS Virtual Edge Serial Number and Interface IP Addresses on page 34 for detailed instructions.
   - **Description** (Optional): Enter a purposeful description for the RUCKUS Edge device.

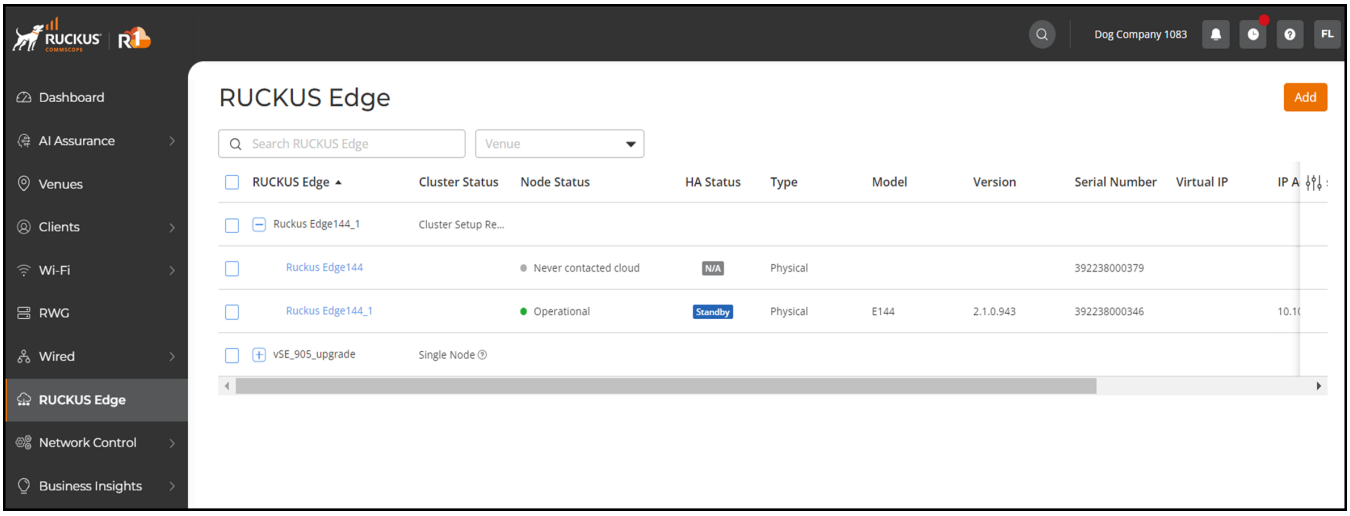
FIGURE 27 Add RUCKUS Edge Device



5. Click **Add**.

   This displays the newly added RUCKUS Edge device on the **RUCKUS Edge** screen.

   FIGURE 28 New RUCKUS Edge Device



NOTE
Upon onboarding to RUCKUS One, the device will automatically upgrade to the latest firmware version associated with the venue.

Adding RUCKUS Edge through the Mobile Application

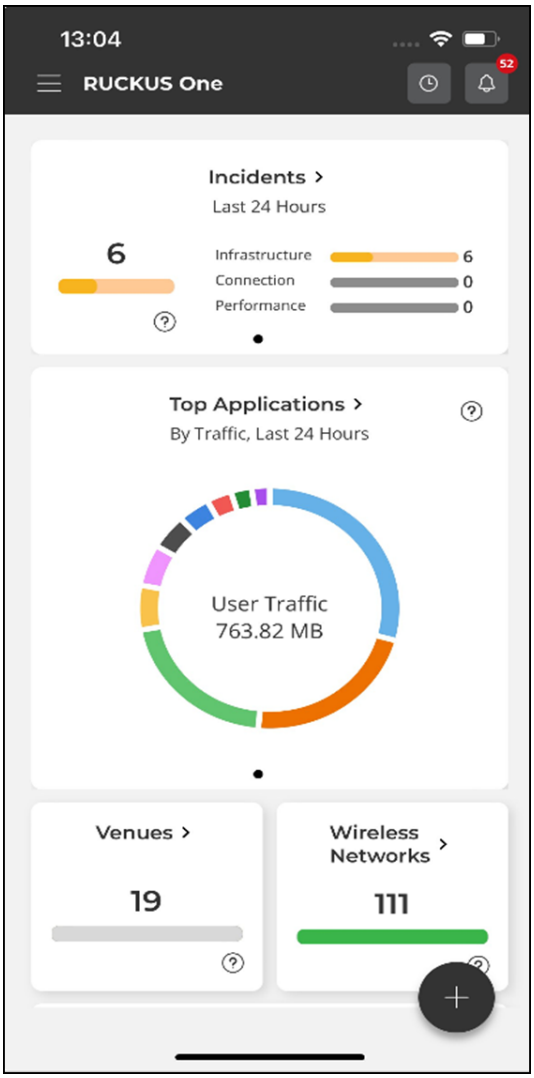
The RUCKUS Edge device must already be successfully installed and deployed on the hypervisor. Refer to Installing and Starting RUCKUS Virtual Edge on the Hypervisor on page 15 for detailed instructions.

To add any RUCKUS Edge device using the RUCKUS One mobile application, download the RUCKUS One application from the **Play Store** (for Google Android phones) or **App Store** (for Apple iPhones).

After downloading the RUCKUS One application on your mobile device, perform the following:

1. Log in to the **RUCKUS One** application with your credentials and select the region from the drop-down menu.
   This displays the **RUCKUS One Dashboard**.

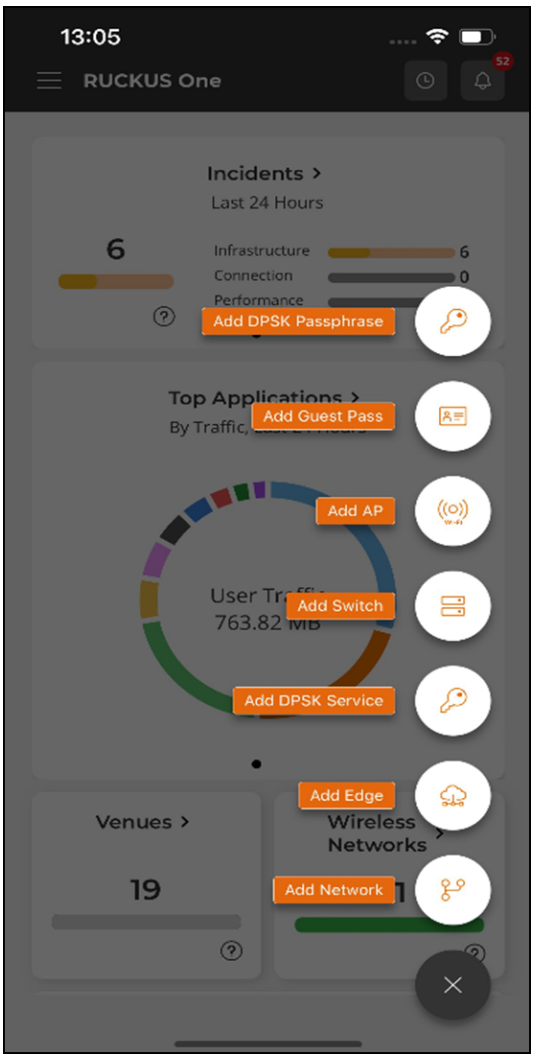
   FIGURE 29 RUCKUS One Dashboard



2. In the **Dashboard**, locate and click ⊕.

   This displays the **Add** menu.

   FIGURE 30 Add Menu



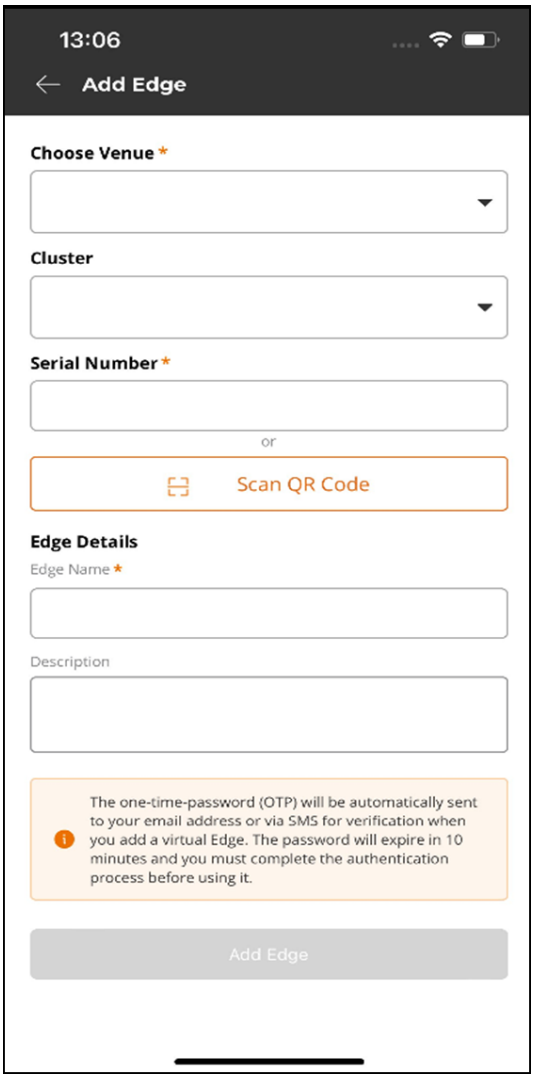
3. Click the **Add Edge** button or icon.

   This displays the **Add Edge** screen.

4. In the **Add Edge** screen, enter the following details:
   - **Choose Venue**: Click the drop-down arrow and choose the venue. A venue represents a physical space where networking devices are deployed.
   - **Cluster**: Click the drop-down arrow and choose the venue to which all traffic is tunneled in the specified venue.
   - **Serial Number**: Enter the serial number of the device or click **Scan QR Code**. The serial number and QR code can be obtained using the VMware ESXi console. Refer to Obtaining the RUCKUS Virtual Edge Serial Number and Interface IP Addresses on page 34 for detailed instructions. If you scan the QR code, **Serial Number** is automatically populated in the field.
   - **Edge Details**: Enter a meaningful name for the RUCKUS Edge device.
   - **Description** (optional): Enter a purposeful description for the RUCKUS Edge device.

   After all required fields are filled, the **Add Edge** button becomes active.

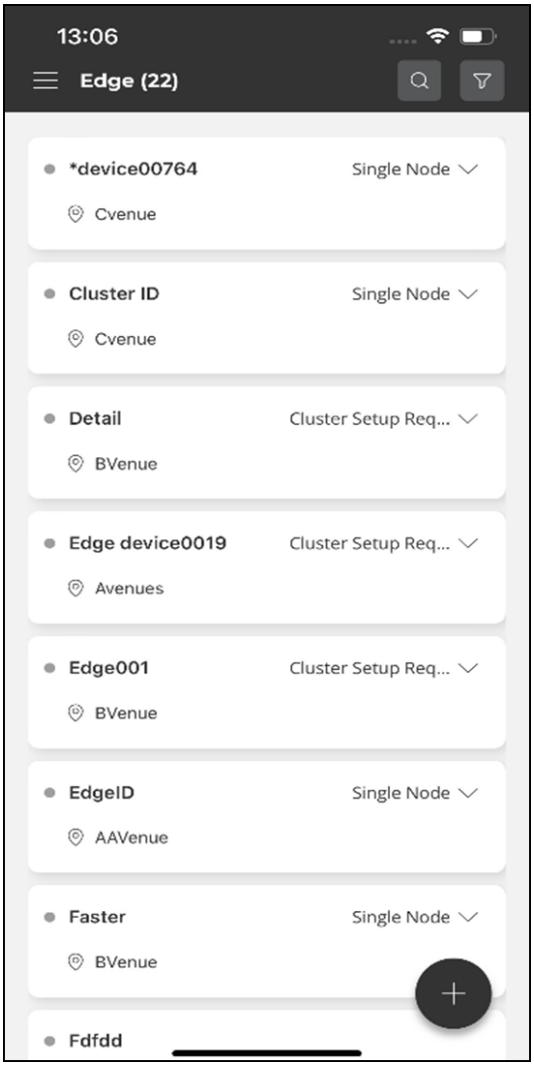
FIGURE 31 Add Edge Details Screen



5. Click **Add Edge**.

   The screen refreshes, showing a list of all RUCKUS Edge devices that have been added.

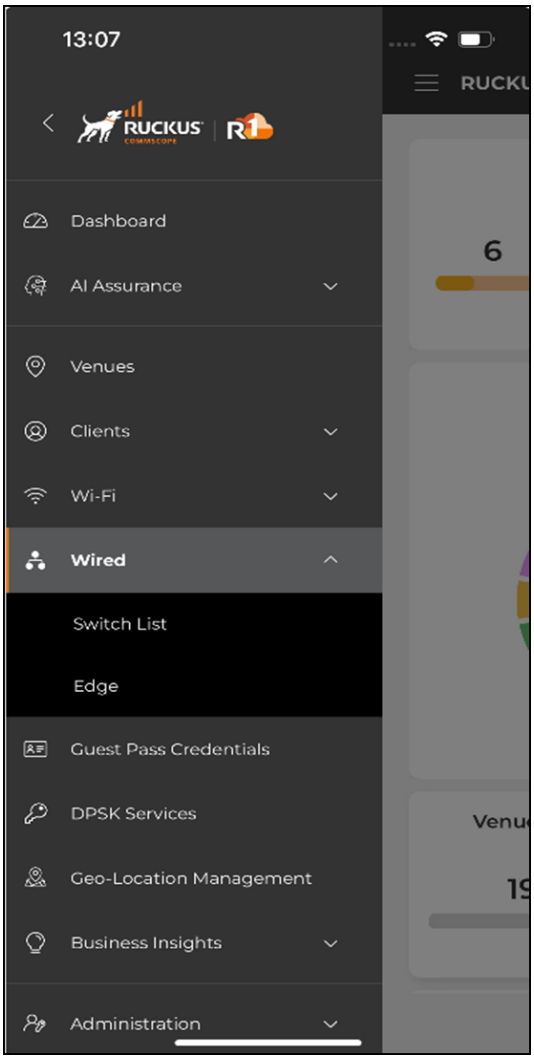
   FIGURE 32 List of Devices on the Edge Screen



6. Click on the device name to view and monitor the RUCKUS Edge. In an operational device you can monitor the following activities:
   - **Overview** - Displays the Edge Status, Traffic by Volume, Resource Utilization, and other activities.
   - **Services** - Displays all the service-related information.
   - **DHCP** - Displays the device-related information such as Ports, Sub Interfaces, and so on.
   - **Timeline** - Displays the Alarms and Events.
   - **Events** - The severity types are defined by color codes. Event types are defined by severity; they are classified as **Critical**, **Major**, **Minor**, **Warning**, and **Informational**.

     NOTE
     At any time, you can view and monitor a specific RUCKUS Edge device by navigating the sidebar menu on RUCKUS One mobile app. Refer to Figure 33.

FIGURE 33 RUCKUS One Mobile Application Sidebar Menu



Authenticating the RUCKUS Virtual Edge Using the OTP

The second step of the RUCKUS Virtual Edge onboarding process is to authenticate and authorize your RUCKUS Virtual Edge device on RUCKUS One.

The RUCKUS Virtual Edge device must already be successfully added to RUCKUS One and have a status of **Never contacted cloud**.

When RUCKUS Virtual Edge is added to RUCKUS One, a one-time password (OTP) for the specific serial number of the device is sent to the email address and phone number registered with theRUCKUS One account. The OTP is valid for ten minutes.

FIGURE 34 Example OTP Email Message

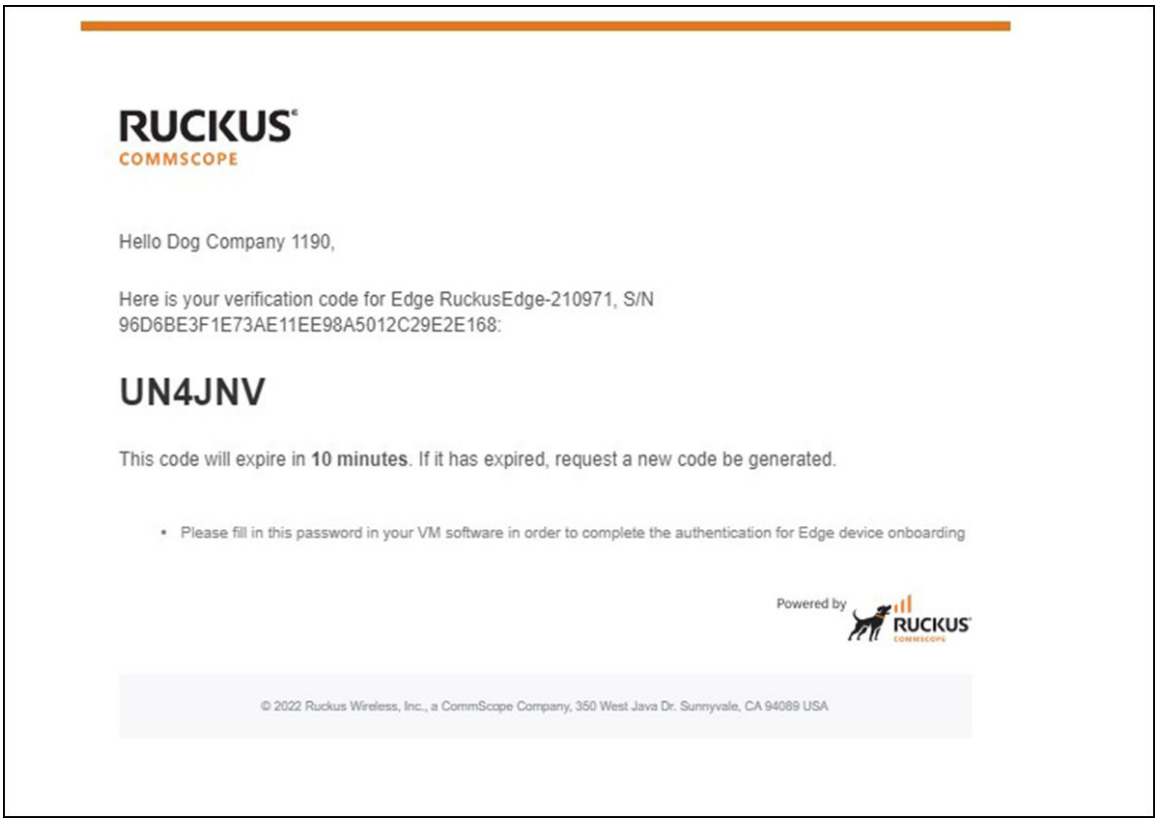
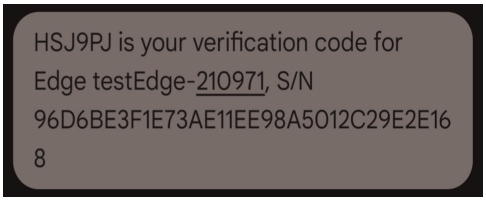


FIGURE 35 OTP Received as an SMS



To complete the onboarding process, perform the following steps to authenticate and authorize the RUCKUS Virtual Edge device for RUCKUS One management.

NOTE
Make sure the RUCKUS Virtual Edge has internet connectivity through one of the connected cables, otherwise, this step fails.

1. After receiving the OTP for the specific device, log in to the RUCKUS Virtual Edge VMware ESXi Console using the credentials: **Username**: admin, **Password**: admin.
2. Enter the **enroll-device** command to initiate the authentication process of the RUCKUS Virtual Edge device with RUCKUS One.

FIGURE 36 enroll-device Command

After you enter the **enroll-device** command, RUCKUS Virtual Edge goes through the following steps:

a. The RUCKUS Virtual Edge negotiates with RUCKUS One, acquires a valid device certificate and/or key, and installs it locally.
b. Using this certificate and/or key, RUCKUS Virtual Edge authenticates and authorizes with RUCKUS One and is onboarded successfully.
c. The RUCKUS Virtual Edge is displayed on RUCKUS One with the status as **Needs Configuration**.

Regenerating the OTP

You have to regenerate the one-time password (OTP) if you have not used the OTP within 10 minutes or if it was entered incorrectly five times.

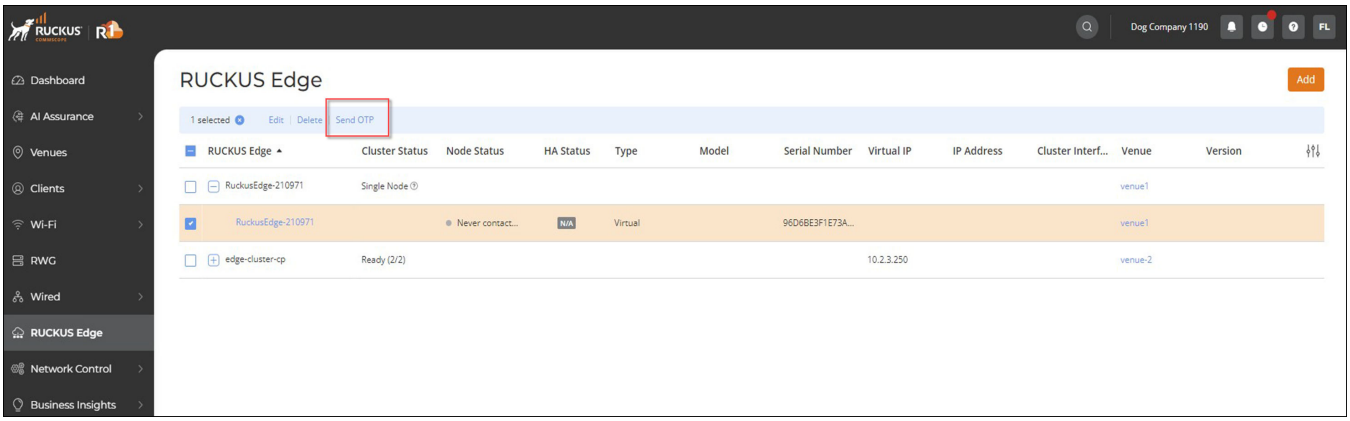
To regenerate the OTP, perform the following:

1. On the RUCKUS One web UI navigation bar, click **RUCKUS Edge**.

   The **RUCKUS Edge** page is displayed.

2. In the **RUCKUS Edge** page, click the checkbox for the RUCKUS Edge device.

   FIGURE 37 Send OTP



3. Click **Send OTP**.

   An OTP is sent to your registered email address and mobile number.

Configuring and Verifying RUCKUS Virtual Edge on RUCKUS One

After the RUCKUS Virtual Edge device is onboarded successfully, the device is displayed on RUCKUS One with the status as **Needs Configuration**. You must configure the interfaces to change the status of the device to **Operational**.

Configuring the Port Details

After the RUCKUS Edge device is onboarded on the RUCKUS One management platform, the status of the RUCKUS Edge and ports is displayed as **Needs Configuration** and **Unconfigured** port type, respectively.

To configure the ports on the RUCKUS Edge device via the RUCKUS One interface, perform the following:

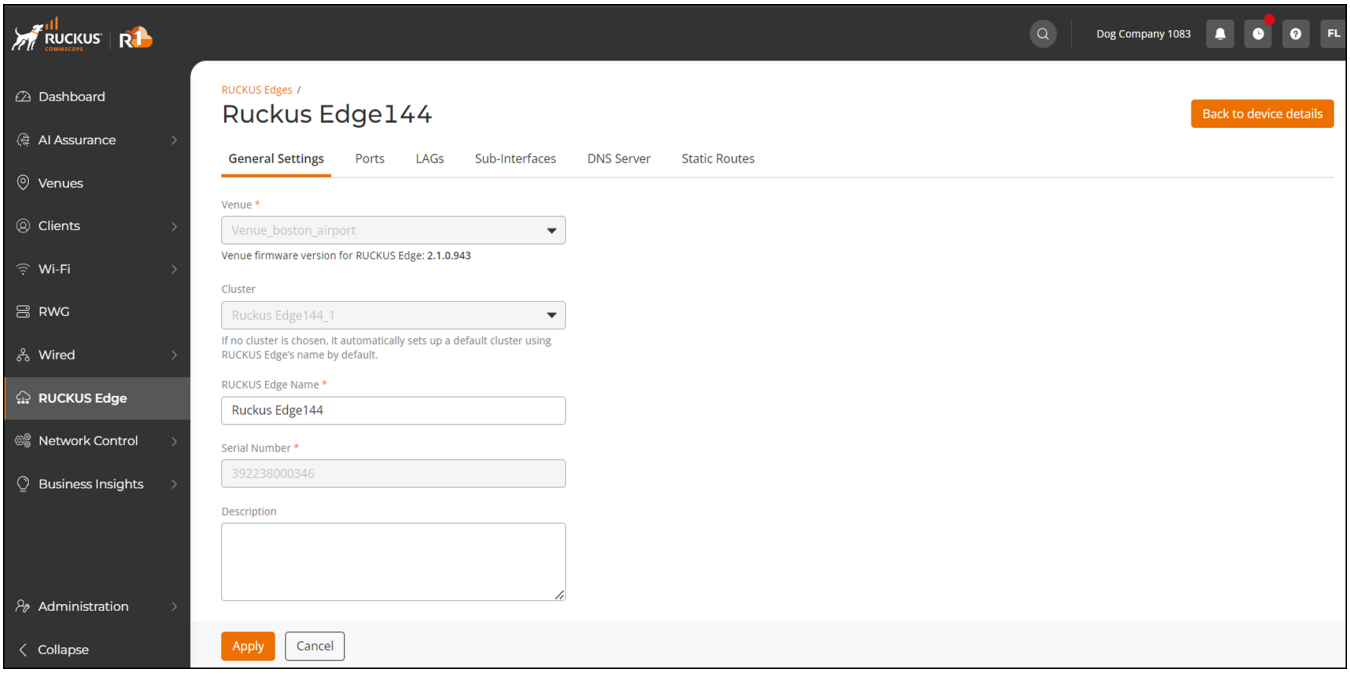
1. Log in to RUCKUS One.
2. On the navigation bar, click **RUCKUS Edge**.

   This displays the **RUCKUS Edge** page.

3. Select a RUCKUS Edge from the list and click **Configure**.

   This displays the **General Settings** tab, by default.

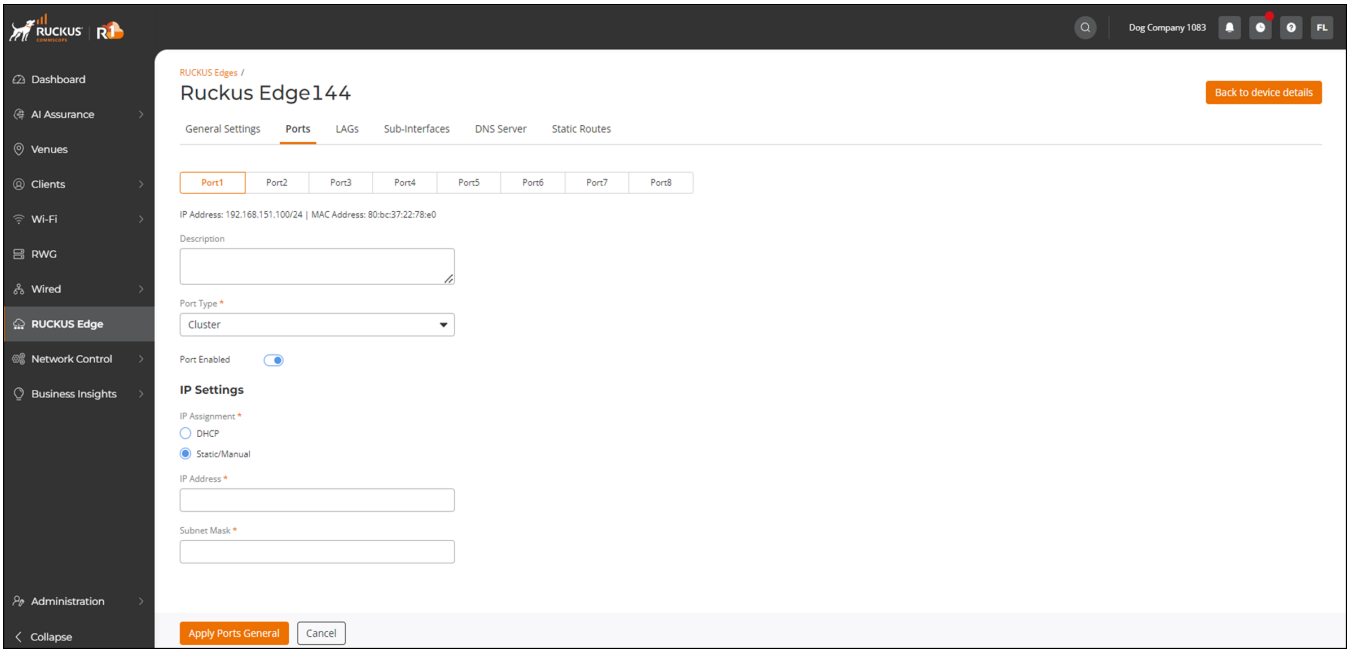
   FIGURE 38 Port Configuration - General Settings



4. Click the **Ports** tab.

   This displays the **Ports** page.

FIGURE 39 Ports Configuration



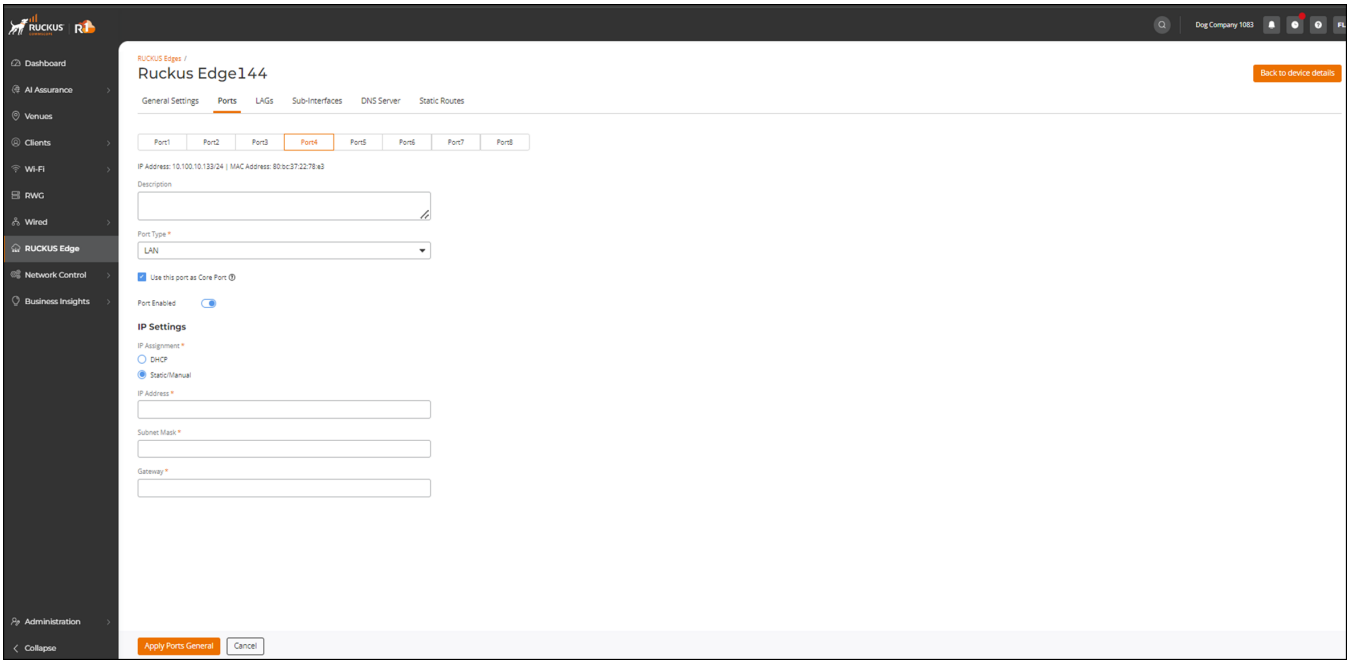
5. In the **Ports** page, configure the following:
   - **Description**: Enter a purposeful statement for **Port1**.
   - **Port Type**: Select the port type as **WAN**, **LAN**, or **Cluster**. Select **LAN** from the drop-down list. This displays **Use this port as Core Port** option.
     - **Use this port as Core Port**: This option utilizes the port for SD-LAN service, the core port on this RUCKUS Edge device establishes a tunnel for directing data transfer effectively.
   - **Port Enabled**: By default, the port is enabled. Click the toggle button to disable the port.

   IP Settings

   - **IP Assignment**
     - **DHCP**: Select the DHCP option to automatically provide the IP host with the device IP address and related configuration.
     - **Static/Manual**: Select the Static/Manual option to and enter the IP details in the fields that appear on the screen.
       - **IP Address**: Enter a valid IP address.
       - **Subnet Mask**: Enter the subnet mask.
       - **Gateway**: Enter the IP gateway address.

         NOTE
         If you are using a static IP, make sure the DNS server IP address is entered. Refer to Configuring the DNS Server on page 57 for details.

FIGURE 40 Port 4 Configuration



6. Click the **Port4** sub-tab and set the required fields. Refer to Step 5 for field descriptions.
7. Click **Apply Ports General**.

   The status of the device is displayed as **Applying Configuration** and then changes to **Operational**.

Configuring a Link Aggregation Group (LAG)

For details on configuring a Link Aggregation Group (LAG) and other related topics, refer to Configuring a Link Aggregation Group in the RUCKUS One User Guide.

Configuring the DNS Server

Manual DNS server configurations are supported at the device level. The DNS server, when configured manually, overrides the server list received from the DHCP option.

1. On the navigation bar, click **RUCKUS Edge**.

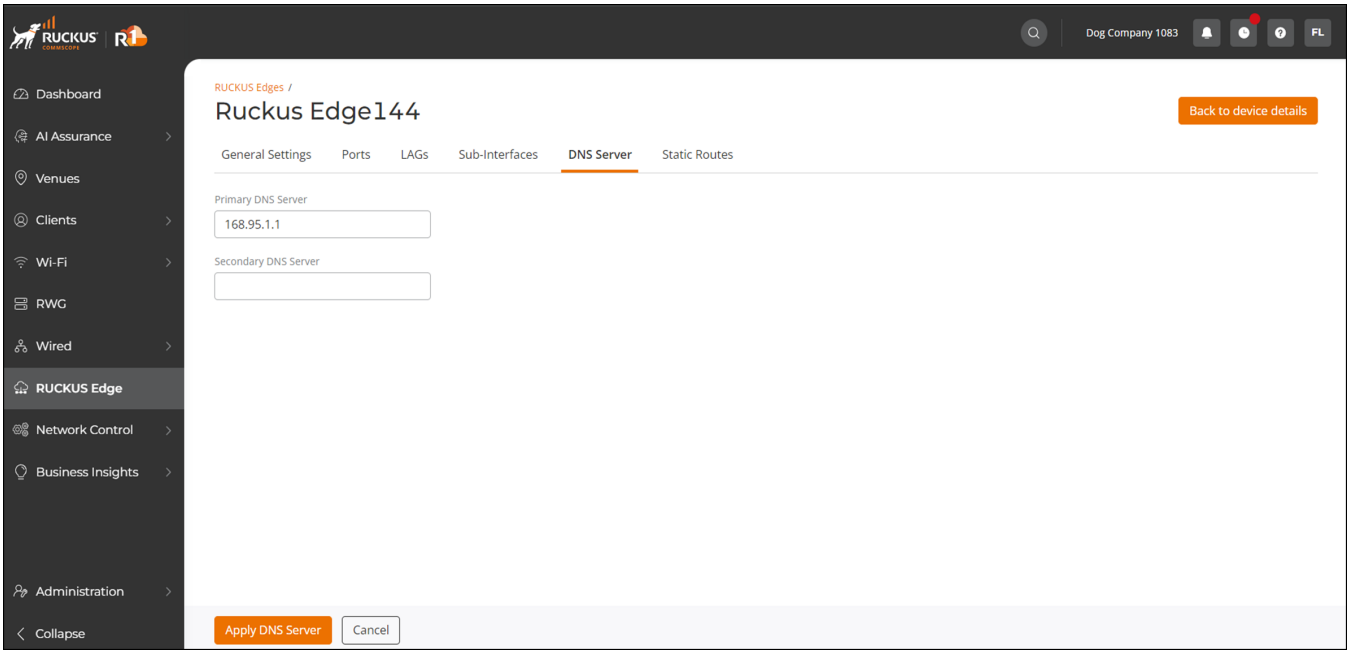
   This displays the **RUCKUS Edge** page.

2. Select a RUCKUS Edge device from the list and click **Configure**.

   This displays the **General Settings** tab, by default.

3. Select the **DNS Server** tab and add the **Primary** and **Secondary** DNS Server IP addresses.

   FIGURE 41 DNS Server



4. Click **Apply DNS Server**.

Configuring Static Routes

Device-level static route configuration is supported at the device level.

If you are using a static IP, make sure the DNS server IP address is entered. Refer to Configuring the DNS Server on page 57 for details.

1. On the navigation bar, click **RUCKUS Edge**.

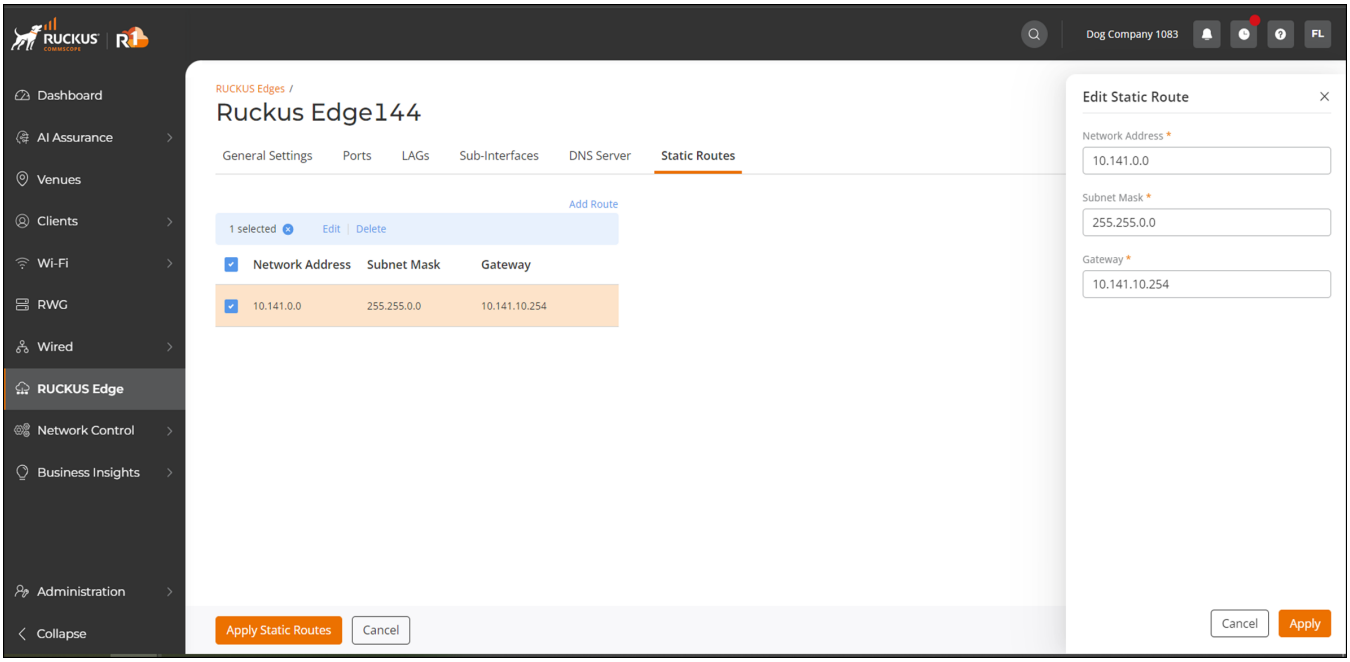
   This displays the **RUCKUS Edge** page.
2. Select a RUCKUS Edge from the list and click **Configure**.

   This displays the **General Settings** tab, by default.
3. Select the **Static Routes** tab and click **Add Route**.

   This displays **Add Static Route** sidebar window.. In this window, enter the following:

   - **Network Address**: Is a host on a communication network. Enter the network IP address.
   - **Subnet Mask**: Is a 32-bit number created by the host. Enter a valid subnet mask.
   - **Gateway**: Is a system between two different networks. Enter a valid gateway address.

   FIGURE 42 Add Static Route



4. Click **Add**.
5. Click **Apply Static Routes**.

Preparing the ESXi Server for vEdge Deployment

Before deploying a RUCKUS Virtual Edge, as a prerequisite you must configure the ESXi host to use Network Time Protocol (NTP) for time synchronization and enable PCI passthrough on the server hardware NIC ports that will be used for vEdge.

Configuring NTP on the ESXi Server

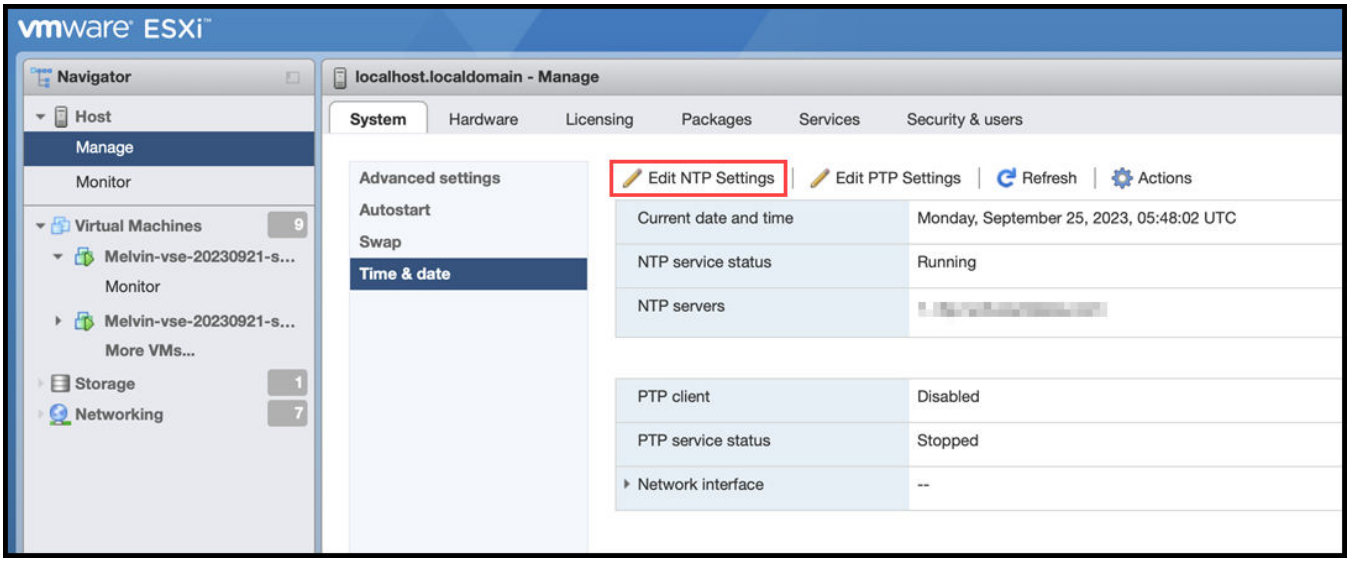
Before deploying a RUCKUS Virtual Edge device, as a prerequisite you must configure Network Time Protocol (NTP) to synchronize the time of the ESXi server with the external NTP server.

Complete the following steps to configure NTP on the ESXi server.

1. Log in to the ESXi server.
2. Select **Host** > **Manage**.
3. Under the **System** tab, select **Time & date** and click **Edit NTP Settings**.

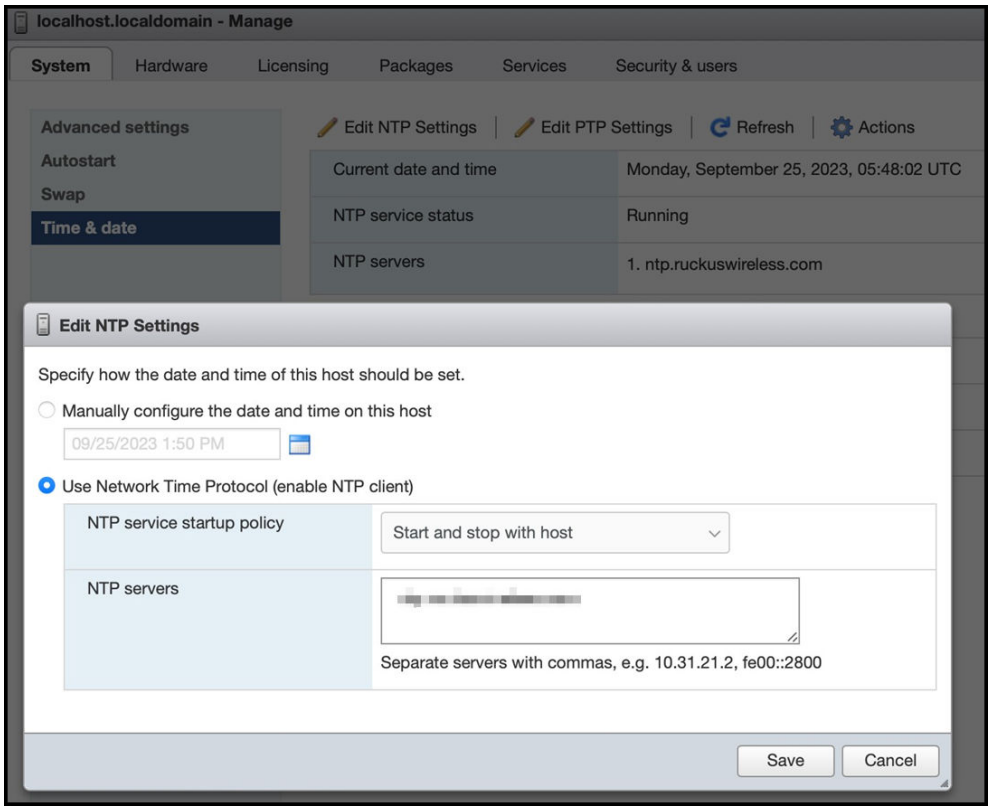
   This displays the **Edit NTP Settings** window.

FIGURE 43 Configuring NTP Settings on the ESXi Server



4. In the **Edit NTP Settings** window, select the **Use Network Time Protocol (enable NTP client)** option.

   FIGURE 44 Editing NTP Settings



5. For **NTP service startup policy**, select **Start and stop with host** from the list.
6. For **NTP servers**, enter the IPv4 or IPv6 address for one or more NTP servers.
7. Click **Save**.

Enabling PCI Passthrough on the ESXi Server

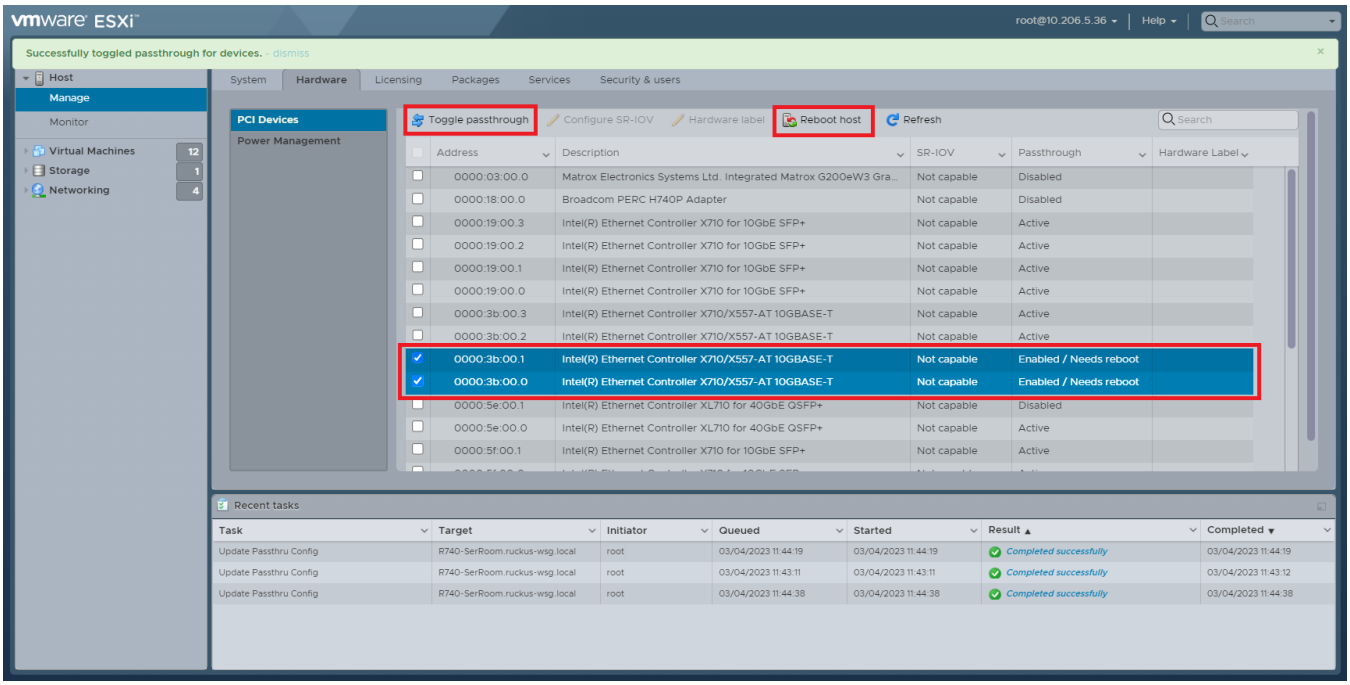
For certain NIC ports, you need to enable PCI passthrough on the ESXi hardware page first. Before enabling or disabling the PCI passthrough, you must reboot the entire ESXi system if the ESXi version is lower than 7.0.

To activate a PCI passthrough interface on a NIC port planned for the RUCKUS Virtual Edge, complete the following steps.

1. On the **ESXi Management** page, click **Manage**.
2. Select the **Hardware** tab.

3. Click **PCI devices** to display all PCI devices on ESXi.

FIGURE 45 PCI Devices



4. Select the NIC ports that you want to use as PCI ports.
5. Click **Toggle Passthrough** to activate PCI mode for selected NIC port.

   The system prompts the user to restart the ESXi system.
6. Click **Reboot host** to restart ESXi.

   The ESXi system reboots.

Configuring vSwitch on the ESXi Server for RUCKUS Edge

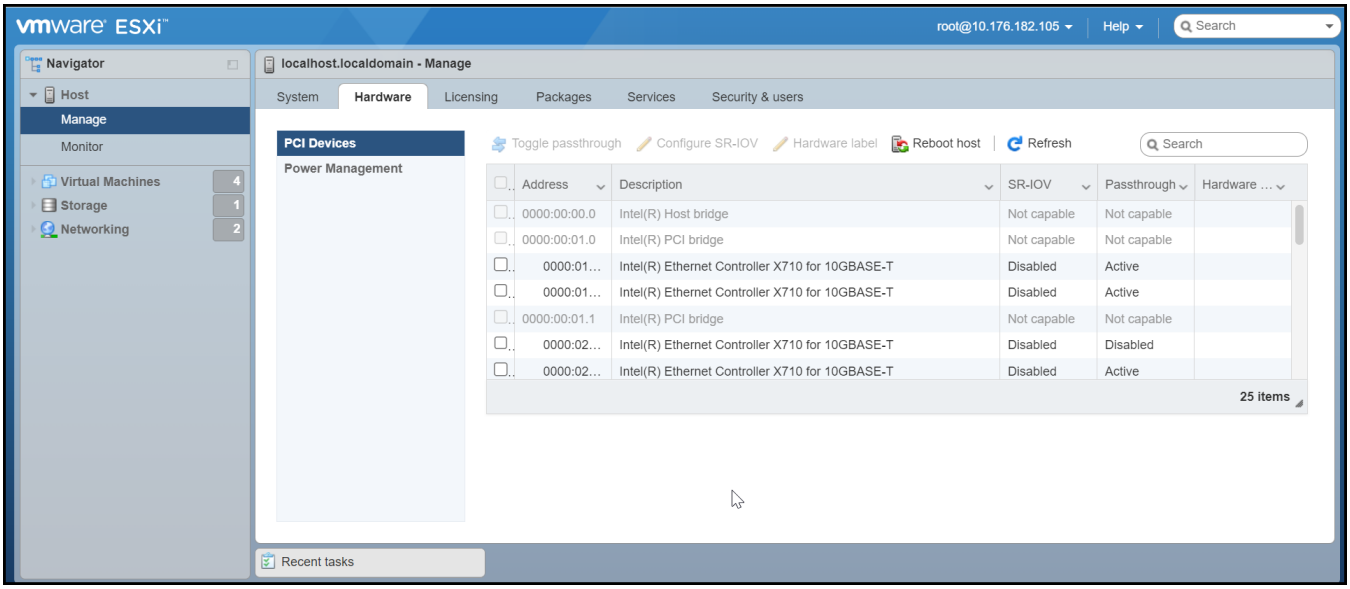
This task comprises configurations on the ESXi server to add a standard virtual switch (vSwitch) on the ESXi server (facilitating vEdge connectivity with the network), add the vSwitch to a port group, and deploy the vEdge and port group.

To configure a vSwitch on the ESXi server for RUCKUS Edge connectivity, perform the following:

1. Log in to the ESXi server.
2. Disable Peripheral Component Interconnect (PCI) passthrough mode on the vEdge NIC ports. In the ESXi **Navigator** menu, select **Host** > **Manage**. Click the **Hardware** tab, then click **PCI Devices**. Select the vEdge NIC ports to disable, then click **Toggle Passthrough**.

   The status displayed in the Passthrough column changes to **Disabled**.

   FIGURE 46 PCI Passthrough Mode Disabled



3. In the ESXi **Navigator** menu, select **Networking** and click the **Virtual switches** tab.

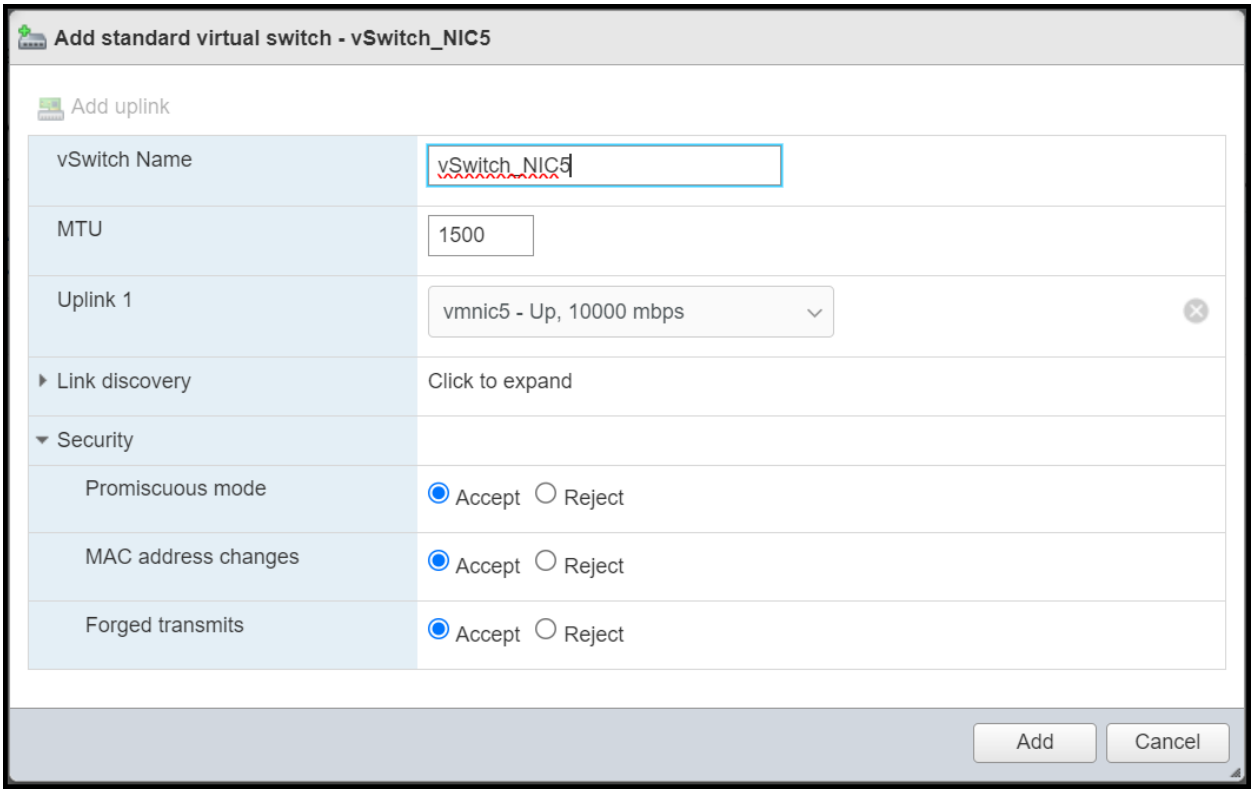
   In the **Virtual switches** window, click **Add standard virtual switch**. This displays **Add standard virtual switch - New switch** window. In this screen, enter the following details:

   - **vSwitch Name**: Enter a name to identify the switch.
   - **MTU**: Maximum Transmission Unit, limits data packet size for any network device. Enter the data packet size limit. The default value is 1500.
   - **Uplink 1**: Uplink port is used to connect the virtual switch to a physical switch. Select the uplink port from the drop-down list.
   - **Link Discovery**: This layer advertises information to directly connected peer/neighbors.
   - **Security**: In this section, the options are to Accept or Reject various security options.

     NOTE
     Accept all the security options.

     - Promiscuous mode: Allows a network device to intercept and read each network packet that arrives in its entirety.
     - MAC address changes: Allows ESXi to accept or reject requests to change the effective MAC address of a virtual machine to a different address than the initial MAC address.
     - Forged Transmits: When accepted, the ESXi server does not check the virtual machine traffic for fake MAC addresses.

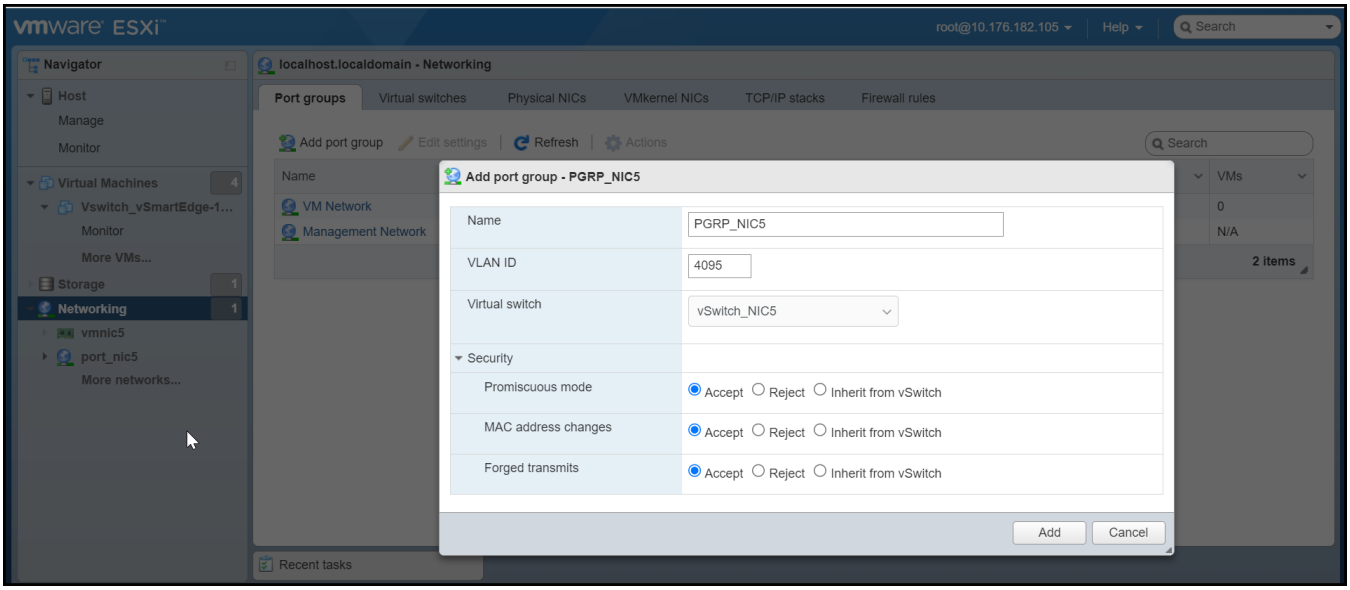
     FIGURE 47 Add Standard Virtual Switch - New Switch



4. Click **Add**. The new vSwitch is added.

5. After creating a new switch, add the switch to the port group. To add the switch, click the **Port groups** tab. This displays the **Add Port Group** window. In this window, enter the following details:
   - Name: Enter a name to identify the port group.
   - VLAN ID: Enter the VLAN ID of the broadcasting domain. For RUCKUS Edge device enter 4095 as VLAN ID.
   - Virtual Switch: Select the configured virtual switch from the drop-down list.
   - Security: Select **Accept** for all options. Refer to the **Add standard virtual switch - New switch** information in Step 3 for descriptions of the Security options and recommended selections.

FIGURE 48 Add Port Group



6. Click **Add**. The new port group is added and associated with the new vSwitch.

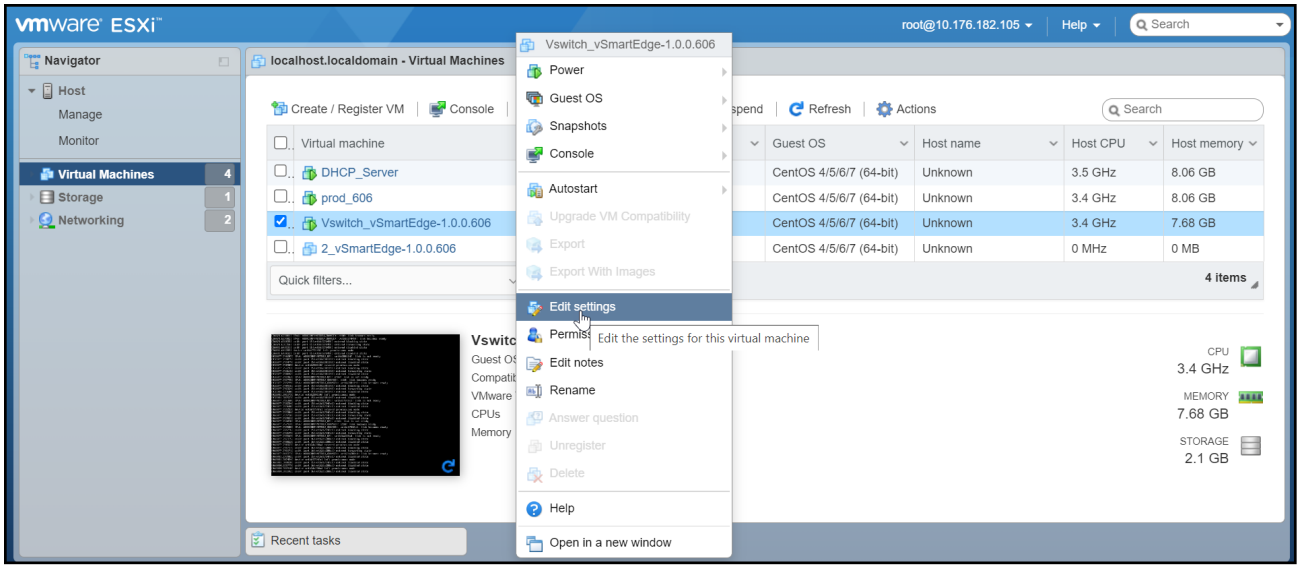
7. After the port group is configured, deploy the vSwitch and the port group by editing the virtual machine settings.

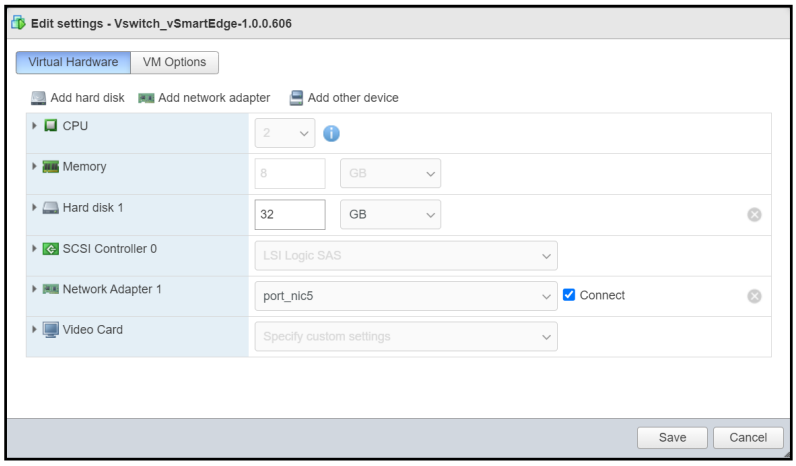
   To edit the virtual machine settings, perform the following:

   a. In the ESXi **Navigator** menu, select **Virtual Machines**.

   b. Right-click on the vSwitch that you just added and select the Edit settings option. This displays **Edit settings** window.

   FIGURE 49 Edit Settings





8. In the **Edit settings** window, click **Add network adapter**.

9. Configure the following network adapter settings:
    - CPU: Select the number of CPUs required for this device.
    - Memory: Select the memory requirement in GB.
    - Hard disk 1: Select the hard disk size in GB.
    - SCSI Controller 0: Select the primary controller for managing SCSI devices.
    - Network Adapter 1: Select the network adapter and select **Connect**.
    - Video Card: Select the video card.
10. Click **Save**.
11. Start the RUCKUS Edge device by right-clicking on the name of your RUCKUS Edge virtual machine and selecting the **Power** option. The interfaces are recognized, and the name is displayed as **VMXNET**.

Configuring Dynamic Resource Allocation

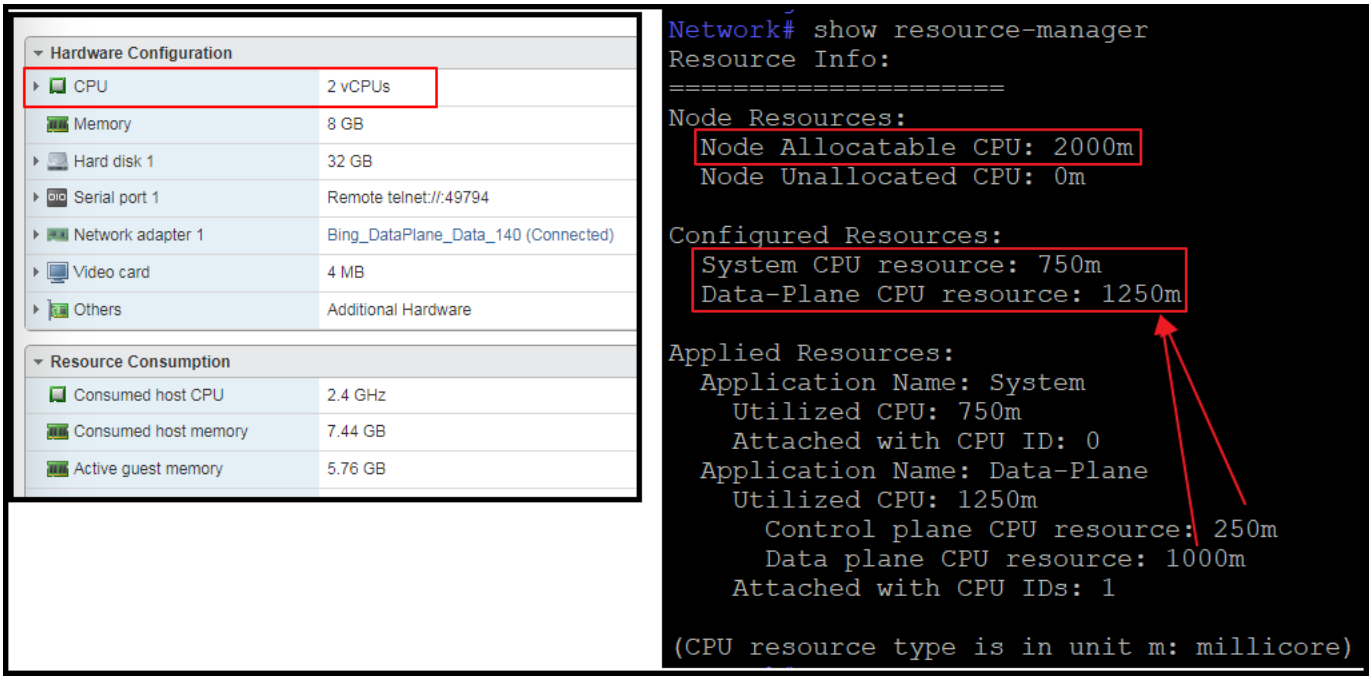
CPU resources are dynamically allocated for RUCKUS Virtual Edge services and applications. You can change the number of CPU resources available for allocation, which will result in automatic adjustments that facilitate optimal utilization of the available resources.

This adjustment process relies on three distinct criteria and selects the optimal combination based on the following factors:

- Network Throughput: Ensuring efficient data transfer rates.
- System Scalability: Adapting to varying system sizes.
- 3rd Party Application Compatibility: Meeting the demands of third-party applications.

The existing default hardware resources bundled with the OVA images consist of 4 CPU cores and 8 GB of memory.

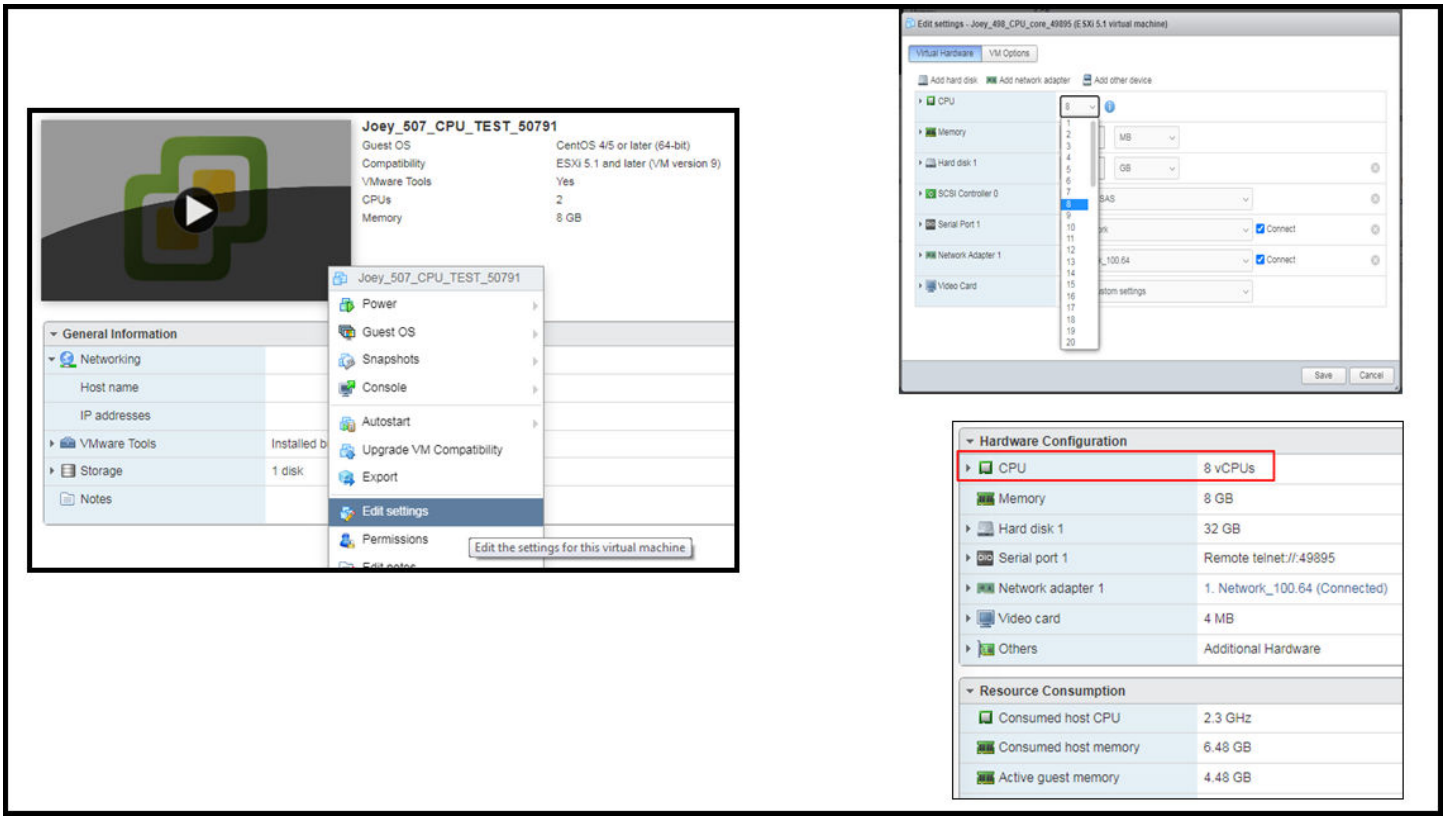
FIGURE 50 Hardware VM CPU resource I



To change the hardware CPU core resource to user-defined cores, such as 8 cores, log in to ESXi and perform the following:

1. In the ESXi **Navigator** menu, select **Virtual Machines**. Right-click on your vEdge virtual machine and select the **Power** option to power-down the vEdge device.
2. Right-click on your Edge virtual machine and select the **Edit settings** option. In the **Edit settings** window, use the drop-down list to modify the **CPU** field. Click **Save** to save and apply the new configuration.
3. Right-click on your Edge virtual machine and select the **Power** option to power-on the Edge device.

FIGURE 51 Hardware VM CPU resource II



350 West Java Dr., Sunnyvale, CA 94089 USA
https://www.commscope.com