VE6120K/VE6125K Virtual Appliances Installation Guide KVM Platform

ExtremeCloud IQ Controller

9037182-00 Rev AC
October 2026



Copyright © 2026 Extreme Networks, Inc. All rights reserved.

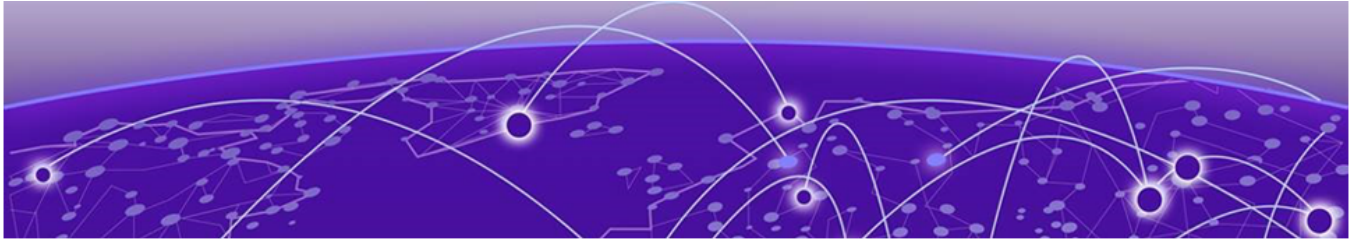


Table of Contents

Legal Notices 5
Legal Notice 5
Trademarks 5
Open Source Declarations 5
Abstract vi

Preface 7
Text Conventions 7
Documentation and Training 8
Open Source Declarations 9
Training 9
Help and Support 9
Subscribe to Product Announcements 10
Send Feedback 10

Overview 11
New in This Guide 11

Virtual Appliance Deployment 12
Deployment Requirements 12
Connectivity Requirements 13
Download a VE6120K/VE6125K Image 14
Install and Deploy the Virtual Appliance Image - Generic Procedure 14
Install and Deploy the Virtual Appliance Image - Proxmox VE Procedure 17

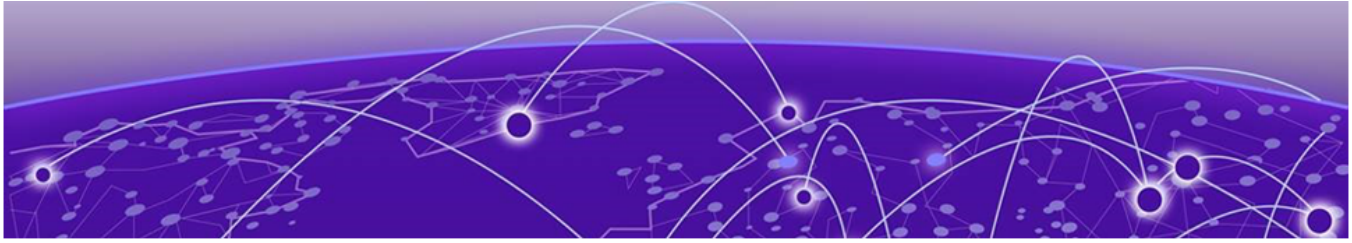
Virtual Appliance Configuration 27
Access the Virtual Appliance Console 27
Configure the VE6120K/VE6125K Using the Basic Configuration Wizard 28
Set up the VE6120K/VE6125K Appliance Using the Basic Configuration Wizard 28
Current Data Port Settings 29
Current Host Attributes 30
Current Global Default Gateway Settings 30
Current Time Settings 30
Upgrade the VE6120K/VE6125K Software 32
Perform a Backup 34
Copy Backup 34
Set Up the Virtual Appliance to Accept USB Flash Drives on a Shutdown VM - Generic Procedure 34
Set Up the Virtual Appliance to Accept USB Flash Drives on a Shutdown VM - Proxmox VE Procedure 35
Set Up the Virtual Appliance to Accept USB Flash Drives on an Operational VM - Proxmox VE Procedure 37
Manage the Flash Memory 38
Remove the Flash Drive - Generic Procedure 39

Remove the Flash Drive from a Proxmox VE Shutdown VM 40
Shut Down and Restart a Virtual Machine Using the Graphical User Interface (GUI) 40
Remove the Flash Drive from a Proxmox VE Operational VM 41
Generate and Install the Activation Package 42
Install the Activation Package 42
Subscription License 42
Shut Down and Restart a Virtual Machine 43
Shut Down and Restart a Virtual Machine Using the Graphical User Interface (GUI) 43
Shut Down and Restart a Virtual Machine on Proxmox VE server 43

Configure Bridges for the Virtual Appliance 45

Create a New Bridge on the KVM Server - Generic Procedure 45
Create a New Bridge on the KVM Server - Proxmox VE Procedure 45
Configure the Bridge for Jumbo Frames Support - Generic Procedure 46
Configure the Bridge for Jumbo Frames Support - Proxmox VE Procedure 46

Index 48



Legal Notices

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

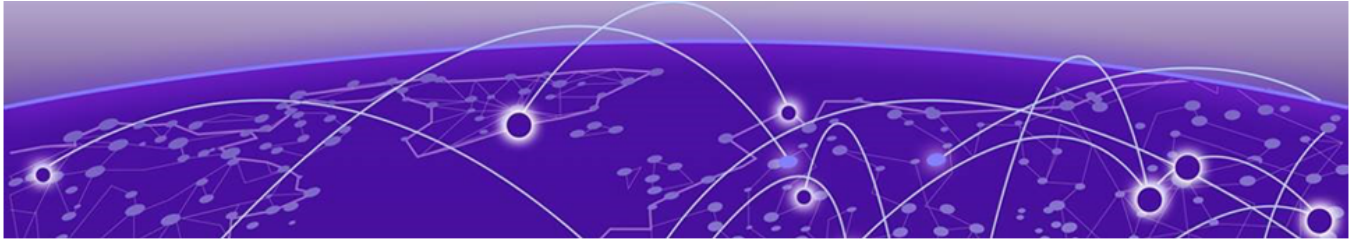
Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see: https://www.extremenetworks.com/about-extreme-networks/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: https://www.extremenetworks.com/support/policies/open-source-declaration/



Abstract

This installation guide for the ExtremeCloud IQ Controller VE6120K and VE6125K Virtual Appliances on the KVM platform covers deployment requirements, VM configuration procedures, initial appliance setup, software upgrade, backup management, USB flash drive integration, licensing, bridge configuration, and VM lifecycle management. The appliances are distributed as compressed raw disk images and must be deployed on a KVM server host; VE6120K and VE6125K use separate images and are not interchangeable. Deployment procedures are provided for both a generic KVM approach and Proxmox Virtual Environment (Proxmox VE), covering VM creation parameters including CPU, memory, disk, and network interface configuration. Scale options range from Small (50 APs, 4 cores, 8 GB RAM) to XLarge (2000 APs, 20 cores, 32 GB RAM), with high-availability pair configurations supporting up to 4000 APs and 32,000 simultaneous users. Initial configuration is performed via the CLI-based Basic Configuration Wizard, which steps through admin password setup, data port settings, host attributes, default gateway, and NTP configuration. Data plane bridges must support promiscuous mode and unmodified VLAN tag forwarding; jumbo frame support requires setting MTU to 1800 bytes on both the network device and attached Linux bridge. USB flash drives, formatted as FAT32, can be attached to both shutdown and operational VMs for backup, restore, upgrade, and log collection. Licensing uses a subscription model tied to managed AP count, with an Activation Package generated from the Extreme Support Portal using a system Locking ID.

Preface

Read the following topics to learn about:

- The meanings of text formats used in this document.
- Where you can find additional information and help.
- How to reach us with questions and comments.

Text Conventions

Unless otherwise noted, information in this document applies to all supported environments for the products in question. Exceptions, like command keywords associated with a specific software version, are identified in the text.

When a feature, function, or operation pertains to a specific hardware product, the product name is used. When features, functions, and operations are the same across an entire product family, such as Extreme Networks switches, the product is referred to as *the switch*.

Table 1: Notes and warnings

Icon	Notice type	Alerts you to...
	Tip	Helpful tips and notices for using the product
	Note	Useful information or instructions
	Important	Important features or instructions
	Caution	Risk of personal injury, system damage, or loss of data
	Warning	Risk of severe personal injury

Table 2: Text

Convention	Description
`screen displays`	This typeface indicates command syntax, or represents information as it is displayed on the screen.
The words *enter* and *type*	When you see the word *enter* in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says *type*.
Key names	Key names are written in boldface, for example **Ctrl** or **Esc**. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press **Ctrl**+**Alt**+**Del**
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
italic text	Italic text indicates variable content.
`[ ]`	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, such as passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*`[`*member*`...]`.
\	In command examples, the backslash indicates a “soft” line break. When a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Documentation and Training

Find Extreme Networks product information at the following locations:

Current Product Documentation
Release Notes

Hardware and Software Compatibility for Extreme Networks products
Extreme Optics Compatibility
Other Resources such as articles, white papers, and case studies

Open Source Declarations

Some software files have been licensed under certain open source licenses. Information is available on the Open Source Declaration page.

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit the Extreme Networks Training page.

Help and Support

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

The Hub

A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2800. For the support phone number in your country, visit www.extremenetworks.com/support/contact.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribe to Product Announcements

You can subscribe to email notifications for product and software release announcements, Field Notices, and Vulnerability Notices.

1. Go to The Hub.
2. In the list of categories, expand the **Product Announcements** list.
3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

You can modify your product selections or unsubscribe at any time.

Send Feedback

The User Enablement team at Extreme Networks has made every effort to ensure that this document is accurate, complete, and easy to use. We strive to improve our documentation to help you in your work, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information.
- Broken links or usability issues.

To send feedback, email us at Product-Documentation@extremenetworks.com.

Provide as much detail as possible including the publication title, topic heading, and page number (if applicable), along with your comments and suggestions for improvement.

Overview

New in This Guide on page 11

The guide describes how to configure and deploy the ExtremeCloud IQ Controller VE6120K and VE6125K Virtual Appliances. This guide is a reference for system administrators who install and manage the VE6120K and VE6125K Virtual Appliances.

Any administrator performing tasks described in this guide must have an account with administrative privileges.



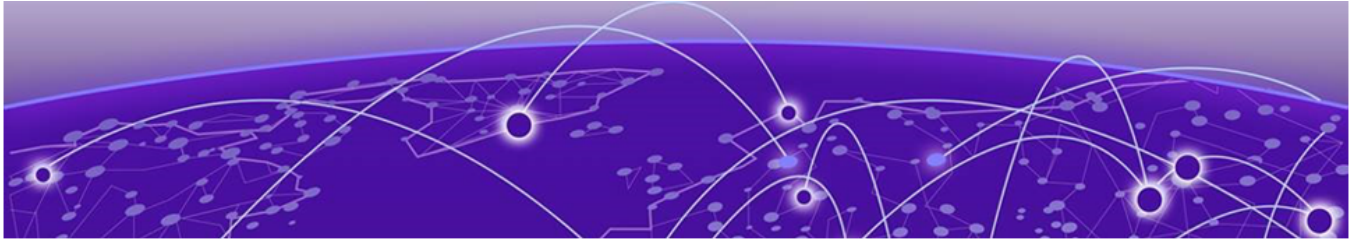
Note
Different Linux distributions use different approaches to create and configure KVM virtual machines (VMs). This document will cover generic steps as well as specific examples for the Proxmox Virtual Environment (Proxmox VE) distribution.

New in This Guide

The following sections show the recent documentation revisions for this guide. Use this information to locate the latest updates.

Table 4: October 2026

Section	Description
Deployment Requirements	Removed Total Switches Managed per Appliance from the table.



Virtual Appliance Deployment

Deployment Requirements on page 12
Connectivity Requirements on page 13
Download a VE6120K/VE6125K Image on page 14

This section provides an overview of the requirements for the ExtremeCloud IQ Controller Virtual Appliances VE6120K and VE6125K deployments. It explains how to install the appliances on a KVM server.

Deployment Requirements

The VE6120K or VE6125K are distributed in the compressed raw disk images for the manually configured KVM virtual machine (VM). The appliances must be deployed on a KVM server host.

Note
VE6120K and VE6125K use separate deployment raw images. You cannot upgrade from VE6120K to VE6125K.

Note
You only need to deploy raw images when you first create the appliance VM. All subsequent upgrades can be performed using the standard controller upgrade procedure to apply a .dve file to the VE6120K appliance and .mfe file for the VE6125K appliance.

In addition, the appliances are configured with one Ethernet interface for administration and two data plane Ethernet interfaces for forwarding payload traffic.

The best practice is to connect them to separate bridges in the host server.

Configuration Options:

Table 5: Virtual ExtremeCloud IQ Controller (VE6120K and VE6125K)

Extreme Application	VE6120K			VE6125K
	Small	Medium	Large	X-Large
Total APs managed in Standalone mode	50	250	500	2000

Table 5: Virtual ExtremeCloud IQ Controller (VE6120K and VE6125K) (continued)

Extreme Application	VE6120K			VE6125K
Additional APs supported in high-availability mode	50	250	500	2000
Total managed APs per Appliance Pair	100	500	1000	4000
Total simultaneous users in Standalone mode	1,000	4,000	8,000	16000
Additional simultaneous users in high-availability mode	1,000	4,000	8,000	16000
Total Simultaneous Users per Appliance Pair	2,000	8,000	16,000	32000
Hardware Requirements				
CPU	4	6	8	20 cores
RAM (GB)	8	16	24	32
Hard Disk (GB)	80	80	80	250

- Consult KVM for minimum host performance requirements for virtual environment. Performance depends on network interface characteristics of underlying host and on utilization on shared interfaces by other virtual appliances.
- Host with 10 Gbps networking connections for data plane interfaces is recommended for best results on Large and XLarge VM profiles.

Connectivity Requirements

The appliances have one management interface (Admin) and two data plane interfaces (Port1, Port2).



Tip
The best practice is to connect to separate external bridges in the host.

The data plane interfaces have additional requirements on the bridges to which they connect:

- The bridge must accept promiscuous mode connections.

- The bridge must accept any VLAN tag traffic and forward it without changing or removing the VLAN tags.



Tip
The best practice is to configure the necessary bridges before installing the appliance.

For more information, see Configure Bridges for the Virtual Appliance for instructions on how to create and configure bridges that can be used by the Virtual Appliance's data plane ports.

Download a VE6120K/VE6125K Image

About This Task

Download the VE6120K-*.raw.xz/VE6125K-*.raw.xz software image to your host.

Procedure

1. Access the VE6120K/VE6125K download page.
2. Download the image from **Downloads > Downloads Home** tab.
   a. Log into the **Downloads Home** using your Extreme Portal login credentials.
   b. Type VE6120K/VE6125K in the search tab and select the search icon. The image list is displayed.
   c. Download the **latest** VE6120K/VE6125K Virtual Appliance image.

Install and Deploy the Virtual Appliance Image - Generic Procedure

About This Task

To install the Virtual Appliance image using the generic procedure:

Procedure

1. Create a virtual machine based on the following parameters:
   - no CD-ROM device
   - OS: Linux, Version: 5.x - 2.6 Kernel
   - Machine: i440fx
   - BIOS: SeaBIOS
   - SCSI Controller: VirtIO SCSI
   - Disk size: 80GB (VE6120K) or 250GB (VE6125K)
   - Disk Cache: Write back
   - Video: none
   - CPU: host

- Cores (socket 1): 4 (VE6120K Small), 6 (VE6120K Medium), 8 (VE6120K Large), or 20 (VE6125K XLarge)

- Memory (MB): 8192 (VE6120K Small), 16384 (VE6120K Medium), 24576 (VE6120K Large), or 32768 (VE6125K XLarge)

- Ballooning Device disabled

- Network

-- net0: Intel E1000, firewall disabled

-- net1: VirtIO (paravirtualized), firewall disabled, multiqueue: 2 (VE6120K) or 4 (VE6125K)

-- net2: VirtIO (paravirtualized), firewall disabled, multiqueue: 2 (VE6120K) or 4 (VE6125K)

- Boot Order: scsi0

- QEMU Guest Agent enabled over VirtIO

- serial console: -chardev socket, id=serial0, port=<**console_port_number**>, host=0.0.0.0, server, nowait, telnet -device isa-serial, chardev=serial0

- watchdog: -device 'i6300esb, bus=pci.0, addr=0×4'

Reference QEMU command line of the VE6120K Small VM:

```
/usr/bin/qemu-system-x86_64 \
  -id 104 \
  -name VE6120K \
  -no-shutdown \
  -chardev 'socket,id=qmp,path=/var/run/qemu-server/104.qmp,server,nowait' \
  -mon 'chardev=qmp,mode=control' \
  -chardev 'socket,id=qmp-event,path=/var/run/qmeventd.sock,reconnect=5' \
  -mon 'chardev=qmp-event,mode=control' \
  -pidfile /var/run/qemu-server/104.pid \
  -daemonize \
  -smbios 'type=1,uuid=c8cfd099-e370-4905-bf83-afa1e628c3ba' \
  -smp '4,sockets=1,cores=4,maxcpus=4' \
  -nodefaults \
  -boot 'menu=on,strict=on,reboot-timeout=1000,splash=/usr/share/qemu-server/
bootsplash.jpg' \
  -vga none \
  -nographic \
  -cpu host,+kvm_pv_eoi,+kvm_pv_unhalt \
  -m 8192 \
  -device 'pci-bridge,id=pci.1,chassis_nr=1,bus=pci.0,addr=0x1e' \
  -device 'pci-bridge,id=pci.2,chassis_nr=2,bus=pci.0,addr=0x1f' \
  -device 'vmgenid,guid=965377a1-862e-4bd4-94f2-96362dd522a7' \
  -device 'piix3-usb-uhci,id=uhci,bus=pci.0,addr=0x1.0x2' \
  -device 'usb-tablet,id=tablet,bus=uhci.0,port=1' \
  -chardev 'socket,path=/var/run/qemu-server/104.qga,server=on,wait=off,id=qga0' \
  -device 'virtio-serial,id=qga0,bus=pci.0,addr=0x8' \
  -device 'virtserialport,chardev=qga0,name=org.qemu.guest_agent.0' \
  -device 'i6300esb,bus=pci.0,addr=0x4' \
  -iscsi 'initiator-name=iqn.1993-08.org.debian:01:c2a1f23f7fc1' \
  -device 'virtio-scsi-pci,id=scsihw0,bus=pci.0,addr=0x5' \
  -drive 'file=/storage/images/104/vm-104-disk-0.raw,if=none,id=drive-
scsi0,cache=writeback,format=raw,aio=threads,detect-zeroes=on' \
  -device 'scsi-hd,bus=scsihw0.0,channel=0,scsi-id=0,lun=0,drive=drive-
scsi0,id=scsi0,rotation_rate=1,bootindex=100' \
```

```
  -netdev 'type=tap,id=net0,ifname=tap104i0,script=/var/lib/qemu-server/pve-
bridge,downscript=/var/lib/qemu-server/pve-bridgedo\
  -device 'e1000,mac=FE:22:F1:81:56:FF,netdev=net0,bus=pci.0,addr=0x12,id=net0' \
  -netdev 'type=tap,id=net1,ifname=tap104i1,script=/var/lib/qemu-server/pve-
bridge,downscript=/var/lib/qemu-server/pve-bridgedo\
  -device 'virtio-net-
pci,mac=06:B5:A9:CB:F3:2E,netdev=net1,bus=pci.0,addr=0x13,id=net1,vectors=6,mq=on' \
  -netdev 'type=tap,id=net2,ifname=tap104i2,script=/var/lib/qemu-server/pve-
bridge,downscript=/var/lib/qemu-server/pve-bridgedo\
  -device 'virtio-net-
pci,mac=E6:A3:20:1B:97:17,netdev=net2,bus=pci.0,addr=0x14,id=net2,vectors=6,mq=on' \
  -machine 'type=pc+pve0' \
  -chardev 'socket,id=serial0,port=56031,host=0.0.0.0,server,nowait,telnet' \
  -device 'isa-serial,chardev=serial0'
```

Reference QEMU command line of the VE6125K XLarge VM:

```
/usr/bin/qemu-system-x86_64 \
  -id 100 \
  -name VE6125K \
  -no-shutdown \
  -chardev 'socket,id=qmp,path=/var/run/qemu-server/100.qmp,server,nowait' \
  -mon 'chardev=qmp,mode=control' \
  -chardev 'socket,id=qmp-event,path=/var/run/qmeventd.sock,reconnect=5' \
  -mon 'chardev=qmp-event,mode=control' \
  -pidfile /var/run/qemu-server/100.pid \
  -daemonize \
  -smbios 'type=1,uuid=07cd719c-fc03-4d3d-ae36-4a612ebf21cf' \
  -smp '20,sockets=1,cores=20,maxcpus=20' \
  -nodefaults \
  -boot 'menu=on,strict=on,reboot-timeout=1000,splash=/usr/share/qemu-server/
bootsplash.jpg' \
  -vga none \
  -nographic \
  -cpu host,+kvm_pv_eoi,+kvm_pv_unhalt \
  -m 32768 \
  -device 'pci-bridge,id=pci.1,chassis_nr=1,bus=pci.0,addr=0x1e' \
  -device 'pci-bridge,id=pci.2,chassis_nr=2,bus=pci.0,addr=0x1f' \
  -device 'vmgenid,guid=42f181ea-8ffe-4d9b-ac0b-1f45ddb07698' \
  -device 'piix3-usb-uhci,id=uhci,bus=pci.0,addr=0x1.0x2' \
  -device 'usb-tablet,id=tablet,bus=uhci.0,port=1' \
  -chardev 'socket,path=/var/run/qemu-server/100.qga,server=on,wait=off,id=qga0' \
  -device 'virtio-serial,id=qga0,bus=pci.0,addr=0x8' \
  -device 'virtserialport,chardev=qga0,name=org.qemu.guest_agent.0' \
  -device 'i6300esb,bus=pci.0,addr=0x4' \
  -iscsi 'initiator-name=iqn.1993-08.org.debian:01:c2a1f23f7fc1' \
  -device 'virtio-scsi-pci,id=scsihw0,bus=pci.0,addr=0x5' \
  -drive 'file=/dev/data2/vm-100-disk-0,if=none,id=drive-
scsi0,cache=writeback,format=raw,aio=threads,detect-zeroes=on' \
  -device 'scsi-hd,bus=scsihw0.0,channel=0,scsi-id=0,lun=0,drive=drive-
scsi0,id=scsi0,rotation_rate=1,bootindex=100' \
  -netdev 'type=tap,id=net0,ifname=tap100i0,script=/var/lib/qemu-server/pve-
bridge,downscript=/var/lib/qemu-server/pve-bridgedo\
  -device 'e1000,mac=4E:FD:02:4C:C5:19,netdev=net0,bus=pci.0,addr=0x12,id=net0' \
  -netdev 'type=tap,id=net1,ifname=tap100i1,script=/var/lib/qemu-server/pve-
bridge,downscript=/var/lib/qemu-server/pve-bridgedo\
  -device 'virtio-net-
pci,mac=2A:39:7A:E0:8E:92,netdev=net1,bus=pci.0,addr=0x13,id=net1,vectors=10,mq=on' \
  -netdev 'type=tap,id=net2,ifname=tap100i2,script=/var/lib/qemu-server/pve-
bridge,downscript=/var/lib/qemu-server/pve-bridgedo\
  -device 'virtio-net-
pci,mac=56:5D:4A:16:63:AF,netdev=net2,bus=pci.0,addr=0x14,id=net2,vectors=10,mq=on' \
  -machine 'type=pc+pve0' \
```

```
  -chardev 'socket,id=serial0,port=56030,host=0.0.0.0,server,nowait,telnet' \
  -device 'isa-serial,chardev=serial0'
```

2. Upload the VE6120K-*.raw.xz/VE6125K-*.raw.xz deployment image obtained in Download a VE6120K/VE6125K Image on page 14 to the KVM server.
3. Uncompress the deployment image over the VM disk image.

   Depending on the selected or configured storage type, it could be a plain disk image file, a LVM storage, or a similar storage option. Check `-drive` parameter in the reference commands in the previous steps for more information.

   Sample commands to populate the disk locations from the examples provided in the previous steps:

   `xz -dc VE6120K-06.01.01.0001.raw.xz > /storage/images/104/vm-104-disk-0.raw`

   `xz -dc VE6125K-06.01.01.0001.raw.xz | dd of=/dev/data2/vm-100-disk-0 bs=1M status=progress`
4. Launch the prepared VM.

Install and Deploy the Virtual Appliance Image - Proxmox VE Procedure

About This Task

Create a virtual machine and configure the virtual machine settings. To install the Virtual Appliance image using the Proxmox VE procedure:

Procedure

1. Log into the Proxmox GUI.
2. In the left pane, select the KVM server host name.
3. Select **Create VM**.
4. Select **Advanced**.
5. Set the desired VM ID and select **Next**.

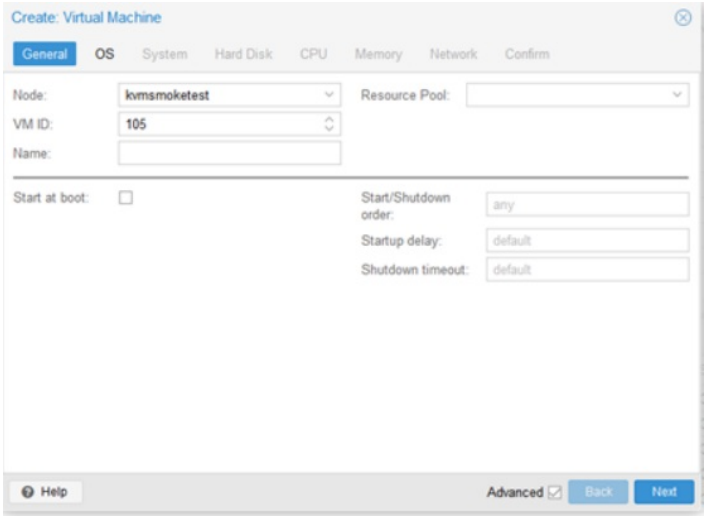


Figure 1: Create: Virtual Machine Window

6. Set the following **OS** configuration and select **Next**:
   a. Select **Do not use any media**.
   b. Set the Guest OS type to **Linux**.
   c. Set the Guest OS version to **5.x–2.6 Kernel**.

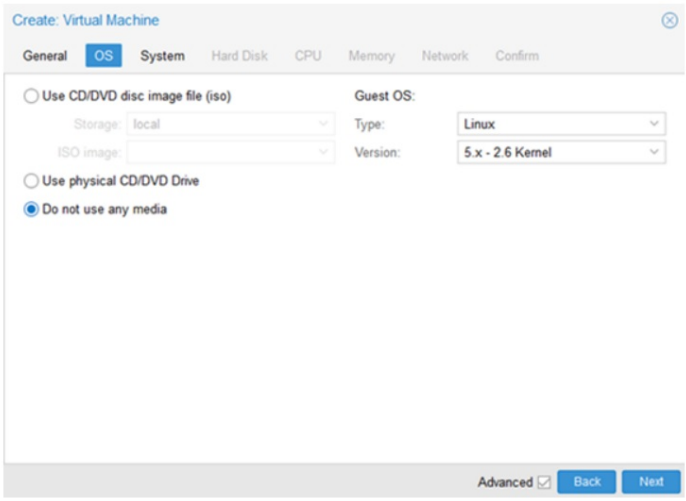


Figure 2: OS Configuration Screen

7. Set the following **System** configuration and select **Next**:
   a. Set the Graphic card option to **none**.
   b. Set the SCSI Controller to **VirtIO SCSI**.
   c. For **Machine**, select **`Default (i440fx)`**.

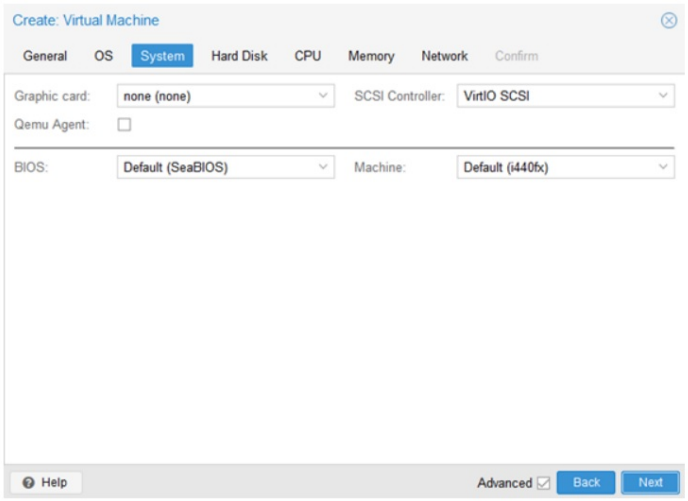


Figure 3: System Configuration Screen

8. Select the appropriate storage available on the server.
9. Set the following **Hard Disk** configuration and select **Next**:
   a. Set the **Disk size (GB)** value to 80 for VE6120K and 250 for VE6125K.
   b. Set the disk image format to **raw**.

c. Select **Write back** for Cache.
d. Select **SSD emulation** if the corresponding storage on the server is SSD based.

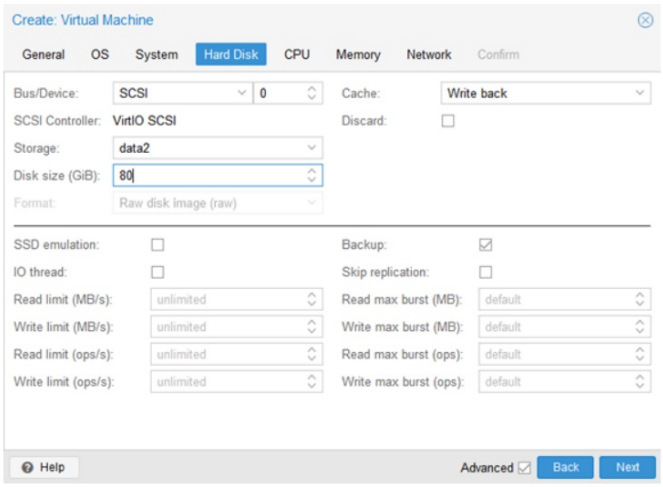


Figure 4: Hard Disk Configuration Screen

10. Set the following **CPU** configuration and select **Next**:
    a. Set the CPU type to **host**.
    b. Set the Cores to **4** for VE6120K Small, **6** for VE6120K Medium, **8** for VE6120K Large, and **20** for VE6125K XLarge (see Deployment Requirements on page 12 for reference).

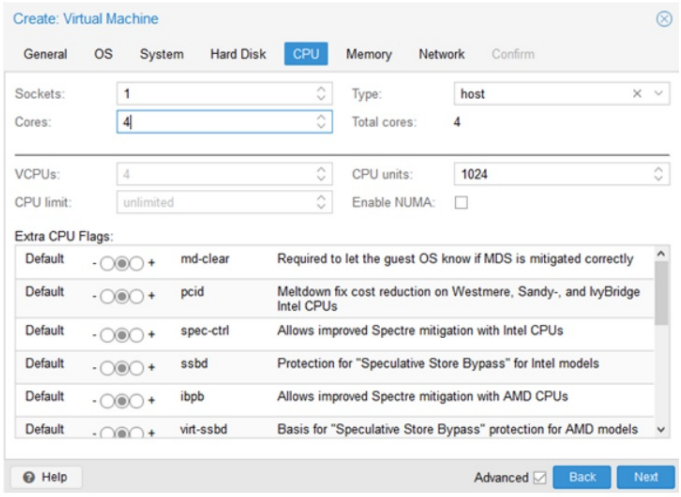


Figure 5: CPU Configuration Screen

11. Clear **Ballooning Device**. Set the following **Memory** configuration and select **Next**:

    Set the **Memory (MiB)** to 8192 for VE6120K Small, 16384 for VE6120K Medium, 24576 for VE6120K Large, and 32768 for VE6125K XLarge.

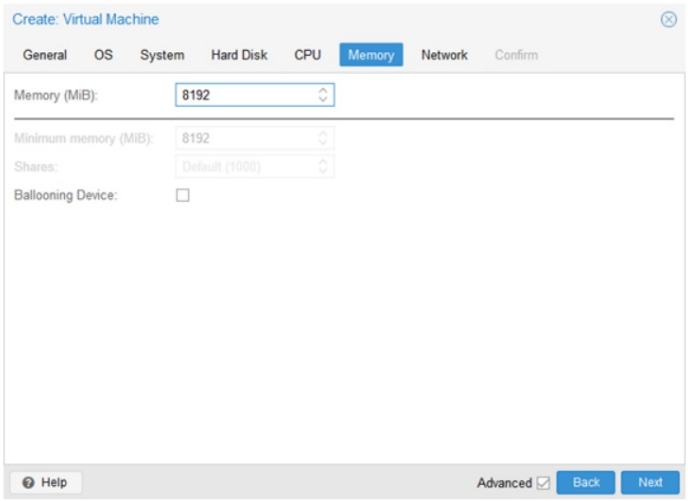


Figure 6: Memory Configuration Screen

12. Set the following **Network** configuration and select **Next**:
    a. Select the **Bridge** for the Admin port.
    b. Set the **Model** as Intel E1000.
    c. Clear **Firewall**.

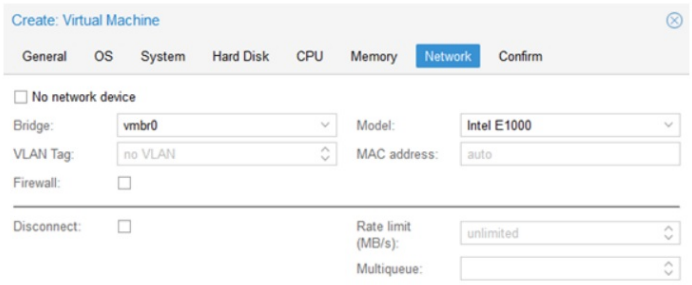


Figure 7: Network Configuration Screen

13. Review the parameters and select **Finish**.

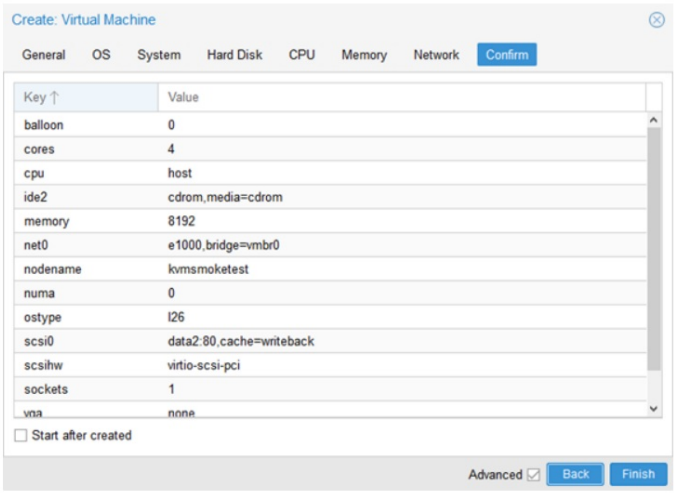


Figure 8: Confirm Screen

Configure the Virtual Machine

About This Task

After you create and configure the virtual machine initial setup, add and configure the networking devices, as well as other additional settings. To apply virtual machine settings:

Procedure

1. Select the virtual machine that you created from the KVM server host name.
2. Select **Hardware**.
3. Select **CD/DVD Drive** > **Remove**.
4. Select **Yes** to confirm removing the CD/DVD Drive entry.

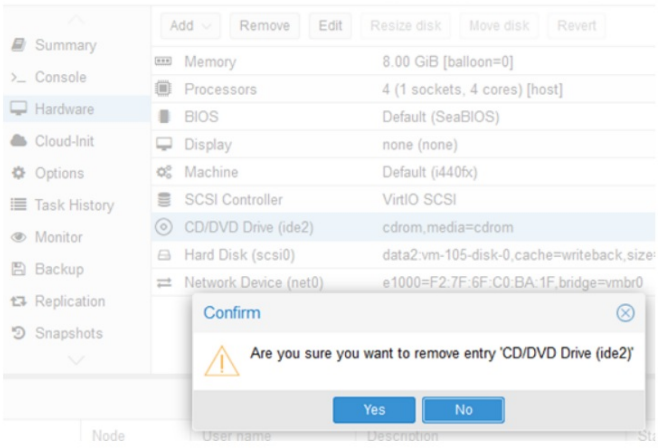


Figure 9: Confirmation Screen

5. Select **Add** > **Network Device** to add data port interfaces.

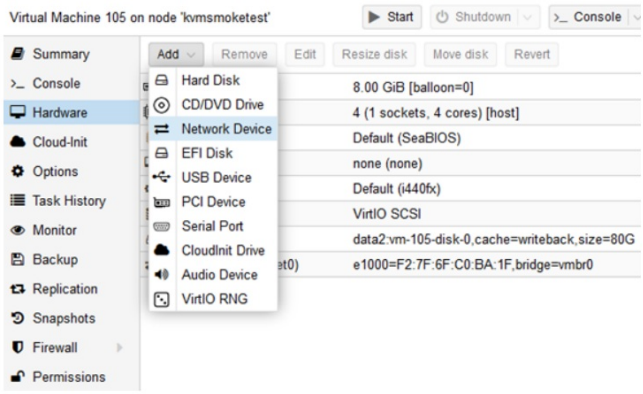


Figure 10: Add Network Device

6. Configure the following **Add: Network Device** settings:
   a. Set the **Bridge** for the first data port interface.
   b. Set the model to **VirtIO (paravirtualized)**.
   c. Clear **Firewall**.
   d. Set Multiqueue to **2** for VE6120K and to **4** for VE6125K.
   e. Select **Add**.

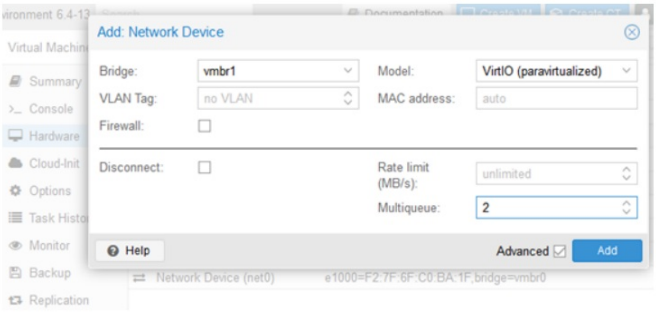


Figure 11: Configure Network Device Settings

7. Select **Add** > **Network Device** again, and select **Bridge** for the second data port interface and configure the other values as described in the previous step.



Figure 12: Select Bridge

8. Select **Options**.

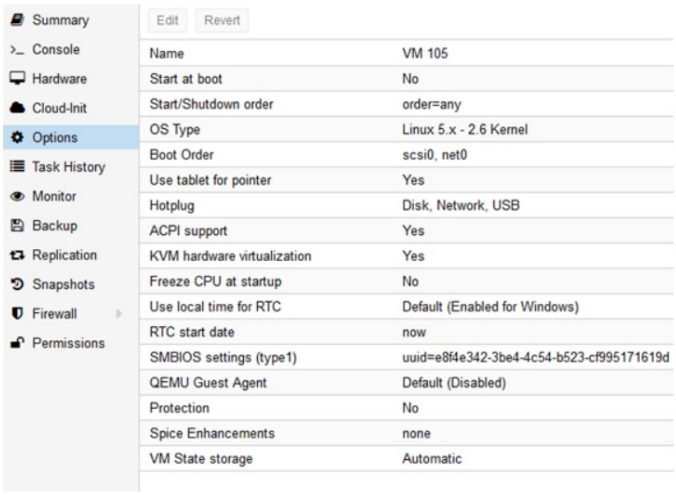


Figure 13: Virtual Machine Options

9. Select **Boot Order** > **Edit**.
10. Clear all the edit options except **scsi0**, and select **OK**.

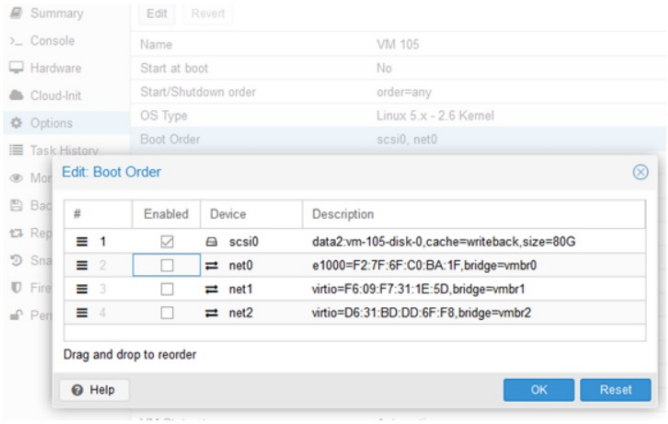


Figure 14: Edit Boot Order

11. Select **Hotplug** > **Edit**.

12. Clear all the edit options except **USB**, and select **OK**.

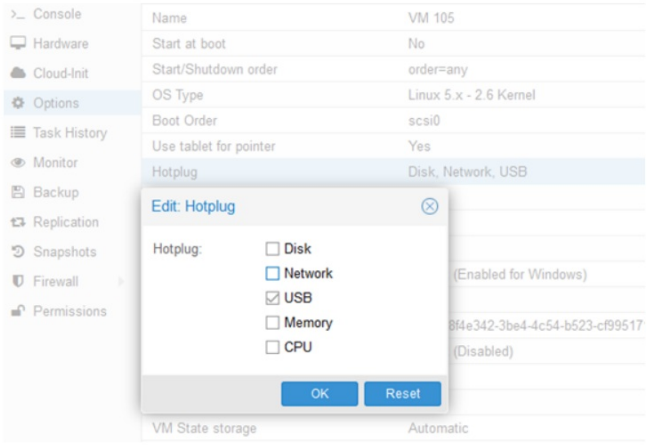


Figure 15: Edit Hotplug Screen

13. Enable QEMU Guest Agent:
    a. Select **QEMU Guest Agent** > **Edit**.
    b. Clear all the edit options except **QEMU Guest Agent**.
    c. Select **VirtIO** for **Type**, and select **OK**.

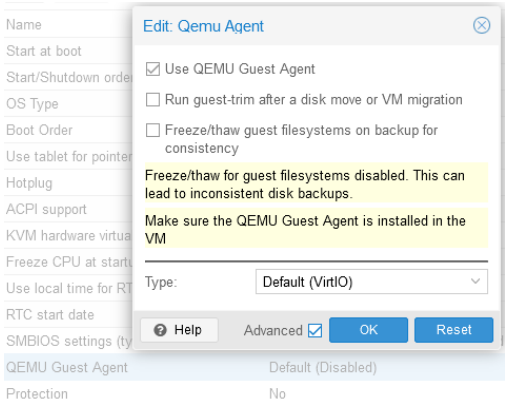


Figure 16: Edit Qemu Agent Screen

Launch the Virtual Machine

About This Task

Perform the following steps to successfully launch a virtual machine. To launch a VM:

Procedure

1. Log into the Proxmox server using secure shell (SSH).
2. Edit the virtual machine configuration file using the following details:

   The virtual machine configuration file is located under `/etc/pve/nodes/<KVM_hostname>/qemu-server/<VM_ID>.conf`, where **KVM_hostname** is the name of the server and **VM_ID** is the virtual machine ID number configured in Step 4.

Edit the VM configuration file to add the following two lines to add serial port and watchdog functionality:

```
args: -chardev
socket,id=serial0,port=<console_port_number>,host=0.0.0.0,server,nowait,telnet -device
isa-serial,chardev=serial0
watchdog: i6300esb
```

The serial port is added and configured for network access on a network port specified in the `<console_port_number>`.

VE6120K Small Proxmox VM configuration file (e.g. <VM_ID>.conf) sample:

```
# cat /etc/pve/nodes/KVMSERVER/qemu-server/102.conf
agent: 1,freeze-fs-on-backup=0
args: -chardev socket,id=serial0,port=56028,host=0.0.0.0,server,nowait,telnet -device
isa-serial,chardev=serial0
balloon: 0
boot: order=scsi0
cores: 4
cpu: host
hotplug: usb
memory: 8192
name: VE6120K
net0: e1000=BA:44:BE:F7:AA:08,bridge=vmbr0
net1: virtio=E2:55:A7:86:0D:FF,bridge=vmbr1,queues=2
net2: virtio=52:AA:44:EB:DC:A0,bridge=vmbr2,queues=2
numa: 0
ostype: l26
scsi0: plain-storage:102/vm-102-disk-0.raw,cache=writeback,size=80G,ssd=1
scsihw: virtio-scsi-pci
smbios1: uuid=7a25ec0b-0d9f-4fde-9fe4-821afa5f396f
sockets: 1
vga: none
vmgenid: 8013433b-e9ed-4249-9604-2c5ebf0a4b74
vmstatestorage: data2
watchdog: i6300esb
```

VE6125K XLarge Proxmox VM configuration file sample:

```
# cat /etc/pve/nodes/KVMSERVER/qemu-server/100.conf
agent: 1,freeze-fs-on-backup=0
args: -chardev socket,id=serial0,port=56030,host=0.0.0.0,server,nowait,telnet -device
isa-serial,chardev=serial0
balloon: 0
boot: order=scsi0
cores: 20
cpu: host
hotplug: usb
memory: 32768
name: VE6125K
net0: e1000=4E:FD:02:4C:C5:19,bridge=vmbr0
net1: virtio=2A:39:7A:E0:8E:92,bridge=vmbr1,queues=4
net2: virtio=56:5D:4A:16:63:AF,bridge=vmbr2,queues=4
numa: 0
ostype: l26
scsi0: data2:vm-100-disk-0,cache=writeback,size=250G,ssd=1
scsihw: virtio-scsi-pci
smbios1: uuid=07cd719c-fc03-4d3d-ae36-4a612ebf21cf
sockets: 1
vga: none
vmgenid: 42f181ea-8ffe-4d9b-ac0b-1f45ddb07698
vmstatestorage: data2
watchdog: i6300esb
```

3. Upload the obtained deployment image (VE6120K-*.raw.xz or VE6125K-*.raw.xz) to the KVM server.
4. Uncompress the deployment image over the VM disk image.

   Depending on the selected or configured storage type, it could be a plain disk image file, a LVM storage, or a similar storage option.

   Use the following example to find the image location:

   `qm showcmd **<VM_ID>** --pretty | grep \\-drive`

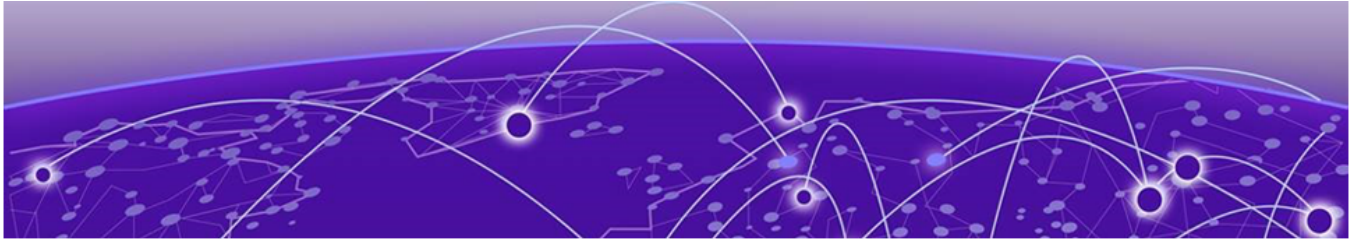
   ```
   # qm showcmd 105 --pretty | grep \\-drive
     -drive 'file=/dev/data2/vm-105-disk-0,if=none,id=drive-
   scsi0,cache=writeback,format=raw,aio=threads,detect-zeroes=on' \

   # qm showcmd 102 --pretty | grep \\-drive
     -drive 'file=/storage/images/102/vm-102-disk-0.raw,if=none,id=drive-
   scsi0,cache=writeback,format=raw,aio=threads,detect-zeroe\
   ```

   Use the following commands to populate the disk locations from the previously mentioned examples:

   ```
   xz -dc VE6125K-06.01.01.0001.raw.xz | dd of=/dev/data2/vm-100-disk-0 bs=1M
   status=progress
   xz -dc VE6120K-06.01.01.0001.raw.xz > /storage/images/102/vm-102-disk-0.raw
   ```

   The VM is ready to launch.
5. On the Proxmox UI, select **VM** > **Start** to launch the VM.



Virtual Appliance Configuration

Access the Virtual Appliance Console on page 27
Configure the VE6120K/VE6125K Using the Basic Configuration Wizard on page 28
Set up the VE6120K/VE6125K Appliance Using the Basic Configuration Wizard on page 28
Upgrade the VE6120K/VE6125K Software on page 32
Set Up the Virtual Appliance to Accept USB Flash Drives on a Shutdown VM - Generic Procedure on page 34
Set Up the Virtual Appliance to Accept USB Flash Drives on a Shutdown VM - Proxmox VE Procedure on page 35
Set Up the Virtual Appliance to Accept USB Flash Drives on an Operational VM - Proxmox VE Procedure on page 37
Manage the Flash Memory on page 38
Remove the Flash Drive - Generic Procedure on page 39
Remove the Flash Drive from a Proxmox VE Shutdown VM on page 40
Remove the Flash Drive from a Proxmox VE Operational VM on page 41
Generate and Install the Activation Package on page 42
Subscription License on page 42
Shut Down and Restart a Virtual Machine on page 43
Shut Down and Restart a Virtual Machine on Proxmox VE server on page 43

After the Virtual Appliance has been deployed on a KVM server using the instructions in Virtual Appliance Deployment on page 12 you are ready to perform initial server configuration.

Access the Virtual Appliance Console

About This Task

To log in to the Virtual Appliance and perform the initial configuration, access the VM console as follows:

Procedure

1. During VM creation, the VM serial port is configured for network access on a particular port.

   To access the console over telnet:

   ```
   telnet <kvm_server_ip> <console_port_number>
   ```

   <kvm_server_ip> is the IP address of the KVM server and **<console_port_number>** is the serial port from the VM serial port configuration.

   Example: telnet 10.0.0.2 55555
2. Type your login credentials:
   - For **User Name**, type `admin`.
   - For **Password**, type `abc123`.

   You now are working in the VE6120K's CLI.

   ```
   root@host:~# telnet 10.0.0.2 55555
   Trying 10.0.0.2...
   Connected to 10.0.0.2.
   Escape character is '^]'.

   ExtremeCloud IQ Controller
   Unauthorized access is prohibited.
   VE6120K.extremenetworks.com login:
   ```

   To end the telnet session, press Ctrl-], and type **quit**.

Configure the VE6120K/VE6125K Using the Basic Configuration Wizard

The ExtremeCloud IQ Controller software provides a Basic Configuration Wizard that can help administrators configure the minimum settings necessary to deploy a fully functioning VE6120K/VE6125K appliance on a network.

Administrators can use the wizard to quickly configure the appliances for deployment, and then after the installation is complete, continue to revise the configuration accordingly.

The wizard is automatically launched when an administrator logs on to the VE6120K/VE6125K CLI for the first time, including after the system has been reset to the factory default settings.

The configuration wizard prompts with a set of **Yes** or **No** questions. The default value is indicated in parenthesis. To accept the default value, press **Enter**.

Set up the VE6120K/VE6125K Appliance Using the Basic Configuration Wizard

About This Task

After logging into the CLI of the VE6120K/VE6125K Basic Configuration Wizard, you will be able to set it up using a set of **Yes** or **No** commands.

Procedure

1. After logging into the CLI of VE6120K/VE6125K, you will be prompted to change the admin password. To begin the admin password setup, press **Enter**.

   The **Admin password Configuration** window opens.

   a. To change the password for the admin account, press **Enter**.
   b. Type the new password for the admin account.

   Note
   The password must have 12–64 characters, including 1 upper case letter (A–Z), 1 lower case letter (a–b), 2 numbers (0–9), and 2 special characters ("^", "$", "#", "@", "!", "%", "&", "*", "(", ")", "-", "=", "_", "+", "|", ",", ".", "/", "<", ">", "?", ";", "~", "[", "]", "{", "}").

   c. Repeat the new password for the admin account and press **Enter**.

      If the passwords match, the password is accepted.
   d. Press **Enter** to accept the changes.

      The **AP access password** window opens.
2. To reset the AP access password, type a new password in the CLI.

   Note
   The password must have 12–64 characters, including 1 upper case letter (A–Z), 1 lower case letter (a–b), 2 numbers (0–9), and 2 special characters ("^", "$", "#", "@", "!", "%", "&", "*", "(", ")", "-", "=", "_", "+", "|", ",", ".", "/", "<", ">", "?", ";", "~", "[", "]", "{", "}").

   a. Retype the AP access password. Select **Enter**.

      Your AP access password is now reset and the **Current Data Port Settings** CLI opens.

Current Data Port Settings

About This Task
When you set up the **Admin Password configuration**, you will be prompted to set up the **Current Data Port Settings**. To set up the data port:

Procedure

1. In the **Current Data Port Settings**, you will determine the port settings. The default port is **Port1**.
2. Select **Enter** to select **Port1**.
3. Set IP Address to the default value. The default value is **`10.0.0.1`**.
4. Press **Enter**.

   The IP Address is selected.
5. Set Netmask to default value of **`255.255.255.0`**.
6. Press **Enter**.

   The Netmask is set.
7. Press **Enter** to set the default VLAN. The tagged frames command opens.
8. Press **Enter** to keep the default tagged frames value to **`No`**.
9. To enable management on the interface, press **Enter** to select the default value, **`Yes`**.

10. To enable device registration, press **Enter** to select the default value, **yes**. The updated Data Port Interface settings open.
11. To accept the changes and keep the data port settings to the values you have chosen, press **Enter**.

    The Data Port Interface is now set. The CLI navigates to the **Current Host Attributes Settings** window.

Current Host Attributes

About This Task

To set up the current host attributes:

Procedure

1. Press **Enter** to change the Host Attributes.
2. Press **Enter** to enter the host name for the application.
3. Type **Y** to set up a dedicated Admin port for out-of-band management. The default option is **no**.

   The following note opens: Admin port does not allow device registration.
4. Type the IP address in the following format **xx.xx.xx.xx** to set up the IP address for the Admin Port.
5. Press **Enter** to accept the default IP netmask for the Admin Port.
6. Press **Enter** to accept the default domain name for the appliance. The default domain name is **extremenetworks.com**.
7. Press **Enter** to configure your Primary DNS server.
8. Type another IP address **xx.xx.xx.xx** to set up the IP address of the Primary DNS and press **Enter**.
9. The default option to set up a Secondary DNS server is **no**. Press **Enter** to accept the default option.

   The updated Host Attribute settings are displayed. To accept the changes you have made, press **Enter**. The **Current Global Default Gateway Settings** CLI opens.

Current Global Default Gateway Settings

About This Task

The global default gateway can be on any Admin or data port topology or subnet.

Procedure

1. Type an IP address.
2. Press **Enter** to accept the changes.

   You are navigated to the **Current Time Settings** CLI.

Current Time Settings

About This Task

The Current Time Settings option allows you to change the time zone as per your location.

Procedure

1. Press **Enter** to change the Time settings.
2. Press **Enter** again if you would like to change the Time Zone. The Region number list is displayed.

   Important
   Ensure that ExtremeCloud IQ Controller is configured with the correct Network Time Protocol (NTP) Server settings. Licensing management and several other system functions are dependent on an accurate timestamp. Configure NTP settings on ExtremeCloud IQ Controller during the initial setup wizard or alternatively under **Administration** > **System** > **Network Time** (as a first configuration step).

3. Pick a number according to the region numbers that is displayed on screen to pick you continent. Then, enter a number that corresponds to the Region. You can enter **n** to move down the list, or **p** to move up the list. To go back to the Region selection, press **c**.
4. Press **Enter** to run NTP as a client.
5. Provide the fully qualified domain name of the NTP server.
6. Press **Enter**.
7. You are prompted to enter a second NTP server and the default option is **y**. Type **n** and press **Enter**.

   NTP Client is enabled.
8. Accept the changes you have made to the time zone and NTP server by pressing **Enter**.

   You are navigated to the **Controller Post Installation Configuration** window along with the menu.

9. If you want to revisit any of the previous windows or exit without applying the configuration changes, enter one of the corresponding numbers or alphabets displayed on screen.

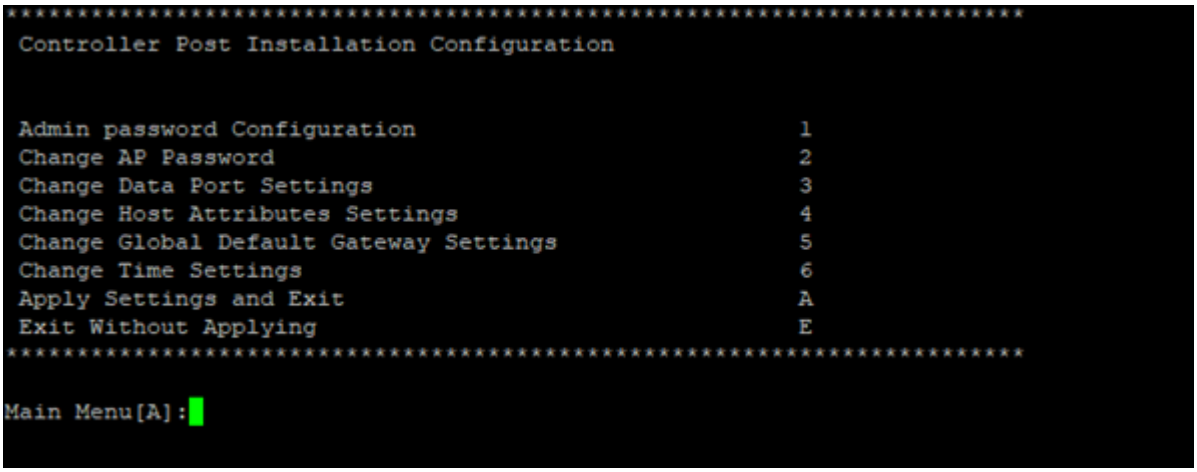


Figure 17: Controller Post Installation Configuration Menu

Table 6: Controller Post Installation Configuration Menu

Menu Option	Command
Admin password Configuration	1
Change AP Password	2
Change Data Port Settings	3
Change Host Attribute Settings	4
Change Global Default Gateway Settings	5
Change Time Settings	6
Apply Settings and Exit	A
Exit Without Applying	E

When you revisit any other screen, you will have to reconfigure all subsequent area settings. For example, if you decide to reconfigure the Admin Password, which is at the beginning of the configuration wizard, you will have to reconfigure all the subsequent configuration wizard settings.

Press **Enter** to accept the settings. The default option for accepting the settings is **A**. Your settings are now applied successfully.

Upgrade the VE6120K/VE6125K Software

About This Task

If you are not installing the **latest** ExtremeCloud IQ Controller release, you need to upgrade the VE6120K/VE6125K software to the latest patch release.

Procedure

1. Go to the Extreme Networks Support site and download the most recent ExtremeCloud IQ Controller software patch.

2. Log in to the virtual appliance using the admin user and password that you configured in the Set up the VE6120K/VE6125K Appliance Using the Basic Configuration Wizard on page 28 section.
3. Go to **Administration > System**.

   The **System** window is displayed.
4. Select **Software Upgrade** tab, and navigate to the **Upgrade** section.
5. To add the image file, select the plus icon.

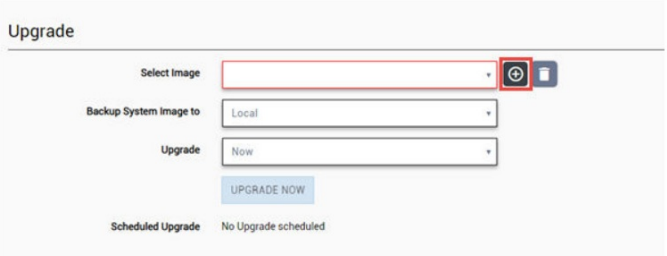


Figure 18: Upgrade Screen

   The **Copy Upgrade Image** window is displayed.
6. To copy an upgrade or backup image to ExtremeCloud IQ Controller, configure the following parameters:

Image Type

Indicates the type of image file used. Valid values are:

- Upgrade
- Backup

Destination

Destination of the uploaded image file:

- Local
- Flash (The Flash drive must be mounted.)

Upload Method

Method used to upload image file to appliance. Valid values are:

- HTTP — Indicates to upload from a local workstation.
- FTP — Indicates to upload from the corresponding server.
- SCP — Indicates to upload from the corresponding server.

When the Upload Method is **FTP** or **SCP**, configure the server properties.

Copy Image from Local Drive

When the Upload Method is **HTTP**, drag image onto ExtremeCloud IQ Controller or select field to navigate to local file directory.

Select Image

Due to a storage space limitation, ExtremeCloud IQ Controller limits the number of locally available upgrade images. If necessary, you can delete an older image before you upgrade to the latest image. To delete an image from ExtremeCloud IQ Controller, from the **Select Image** field, select an image and select .

Perform a Backup

The backup and restore procedure is limited to configuration files and, optionally, logs and audit files. A system backup is a full system snapshot rescue file (*-rescue-user.tgz). Creating a rescue file is an option during the system upgrade process.

Before you perform a backup procedure, decide what to backup and where to save the backup file:

- Select back up configs, logs, and audit or back up configuration only.
- Select a location to store the backup file.
- (Optional) Configure a backup schedule.

On-demand backups can only be stored locally, while scheduled backups can be stored on a mounted flash drive or on a remote server.

Copy Backup

To copy a backup image to ExtremeCloud IQ Controller, configure the following parameters:

Upload Method

Method used to upload file to appliance. Valid values are:

- HTTP — Indicates to upload from a local workstation.
- FTP — Indicates to upload from the corresponding server.
- SCP — Indicates to upload from the corresponding server.

When the Upload Method is **FTP** or **SCP**, configure the server properties.

Copy Image from Local Drive

When the Upload Method is **HTTP**, drag image onto ExtremeCloud IQ Controller or select field to navigate to local file directory.

Set Up the Virtual Appliance to Accept USB Flash Drives on a Shutdown VM - Generic Procedure

Before You Begin

Prepare the Virtual Appliance to accept USB flash drives. The VM must be shut down before adding the USB flash drive.

1. Format the flash drive to FAT32.
2. Insert the flash drive into a USB port on the host.



Note

A USB device is required to be plugged in before it can be added to a virtual machine.

About This Task

The Virtual Appliance can accept USB flash drives. The flash drive can be used for backing up, restoring, upgrading, and collecting log information.

To add a USB flash drive to a shutdown VM:

Procedure

1. Log in to the host using a CLI (for example, SSH) to run the following command:

```
# lsusb
Bus 004 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 003 Device 004: ID 1604:10c0 Tascam
Bus 003 Device 003: ID 1604:10c0 Tascam
Bus 003 Device 002: ID 1604:10c0 Tascam
Bus 003 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 002 Device 002: ID 0424:5744 Standard Microsystems Corp. Hub
Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 001 Device 003: ID 125f:c08a A-DATA Technology Co., Ltd. C008 Flash Drive
```

2. Extend your VM configuration:

   To add the flash drive using USB vendor or device ID:

   Note
   Adjust the **addr** field depending on the devices that are already defined on the PCI bus.

```
-device 'nec-usb-xhci,id=xhci,bus=pci.1,addr=0x1b'
-device 'usb-host,bus=xhci.0,vendorid=0x125f,productid=0xc08a,id=usb0'
```

   Note
   vendorid and **productid** arguments need to match the flash drive ID from the lsusb output.

   To add the flash drive using the USB port:

```
-device 'nec-usb-xhci,id=xhci,bus=pci.1,addr=0x1b'
-device 'usb-host,bus=xhci.0,hostbus=1,hostport=1.3,id=usb0'
```

   Note
   hostbus and **hostport** arguments need to match the flash drive bus and device numbers from the lsusb output.

3. Start the VM.

Set Up the Virtual Appliance to Accept USB Flash Drives on a Shutdown VM - Proxmox VE Procedure

Before You Begin
Prepare the Virtual Appliance to accept USB flash drives. The VM must be shut down before adding the USB flash drive.

1. Format the flash drive to FAT32.
2. Insert the flash drive into a USB port on the host.

   Note
   A USB device is required to be plugged in before it can be added to a virtual machine.

About This Task

The Virtual Appliance can accept USB flash drives. The flash drive can be used for backing up, restoring, upgrading, and collecting log information.

To add a USB flash drive to a shutdown VM:

Procedure

1. Log in to the Proxmox GUI.
2. In the left pane, select the VM from the KVM server host name.
3. Select **Hardware**.
4. Select **Add** > **USB Device**.
   a. To add a flash drive using USB vendor or device ID, select **Use USB Vendor/Device ID**, and choose a device.

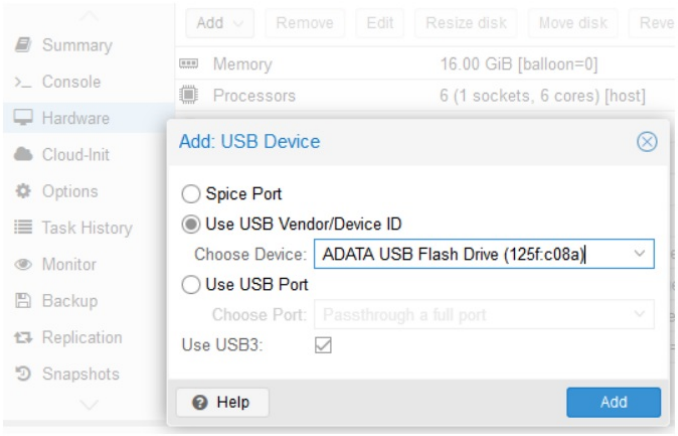


Figure 19: Add USB Device Screen - Use USB Vendor

   b. To add a flash drive using a USB port, select **Use USB Port**, and choose a port.

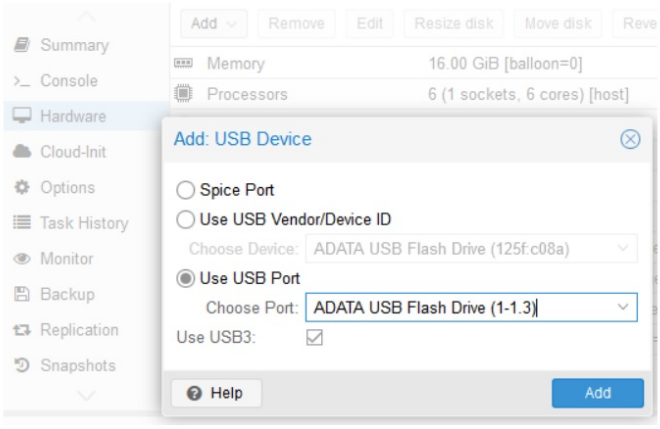


Figure 20: Add USB Device Screen - Use USB Port

5. Select **Add**.

6. Start the virtual machine.

Set Up the Virtual Appliance to Accept USB Flash Drives on an Operational VM - Proxmox VE Procedure

Before You Begin

Prepare the Virtual Appliance to accept USB flash drives.

1. Format the flash drive to FAT32.
2. Insert the flash drive into a USB port on the host.



Note

A USB device is required to be plugged in before it can be added to a virtual machine.

About This Task

The Virtual Appliance can accept USB flash drives. The flash drive can be used for backing up, restoring, upgrading, and collecting log information. A USB drive can be inserted, assigned to a virtual appliance, and removed from the virtual appliance while the appliance is in service.

To set up the VM to accept an USB flash drive when it is operational:

Procedure

1. Log in to the Proxmox GUI.
2. In the left pane, select the VM from the KVM server host name.
3. Select **Monitor**.
4. In the CLI, type **`info usbhost`** to display the list of USB devices available on the host.

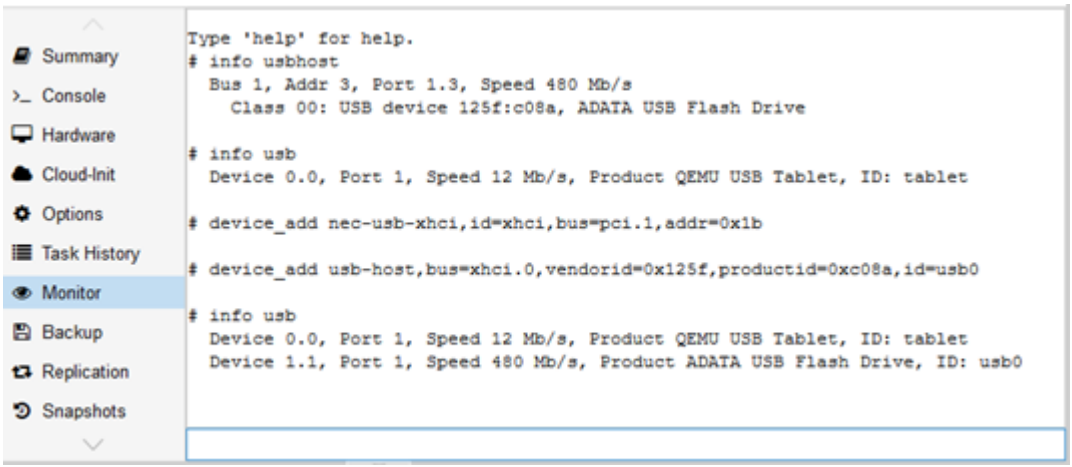
5. Type the following commands:

   `device_add nec-usb-xhci,id=xhci,bus=pci.1,addr=0x1b`

   `device_add usb-host,bus=xhci.0,vendorid=0x125f,productid=0xc08a,id=usb0`

   Note
   The **vendorid** and **productid** arguments need to match the flash drive vendor or device ID from the info usbhost output.

   Adjust the **addr** field depending on the devices already defined on the PCI bus.



6. Type **`info usb`** to verify that the USB device was properly attached to the VM.

Manage the Flash Memory

About This Task
Follow these steps to manage flash memory:

Procedure

1. Log into the ExtremeCloud IQ Controller using your credentials.

2. In the left pane, from the **Administration** drop-down, select **System > Maintenance > External Flash** option.

   Use the **Mount/Unmount** options to mount and unmount flash memory respectively.

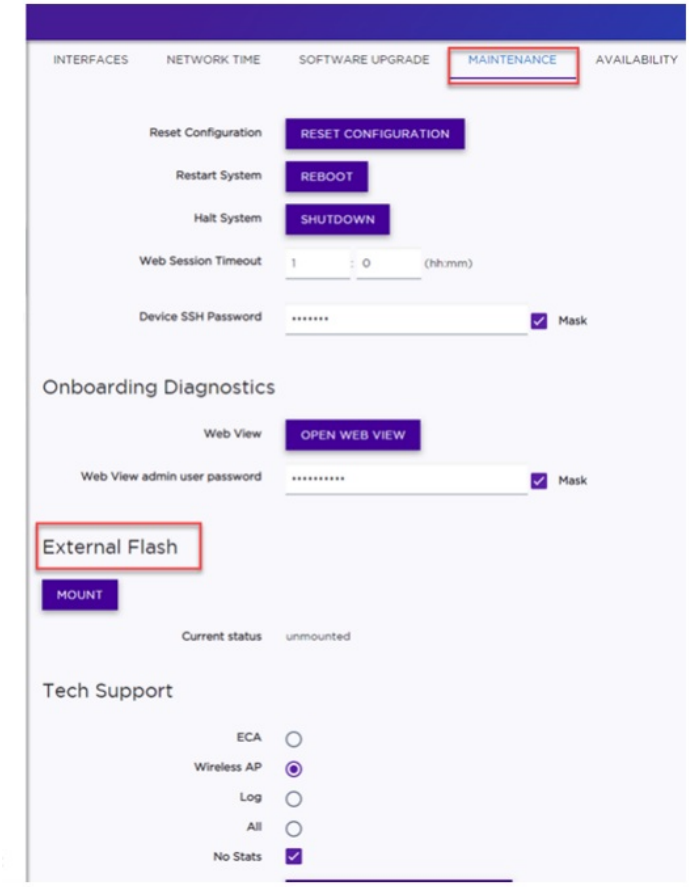


Figure 21: Flash Memory Maintenance Window

Remove the Flash Drive - Generic Procedure

Before You Begin

When you are ready to remove the USB Flash drive, select **Un-Mount** from the Maintenance page.

About This Task

Follow these steps to remove the flash drive.

Note

The Virtual Appliance can be in service when the USB flash drive is assigned to it. Within a few seconds of the USB flash drive being assigned to it, the virtual appliance will detect the flash drive and mount it for use.

Procedure

1. Shut down the virtual machine.

2. Remove the USB device related configuration that was added to the virtual machine.
   For example:
   ```
   -device 'nec-usb-xhci,id=xhci,bus=pci.1,addr=0x1b'
   -device 'usb-host,bus=xhci.0,vendorid=0x125f,productid=0xc08a,id=usb0'
   ```
3. Start the virtual machine.
   The USB flash drive can be removed from the host.

Remove the Flash Drive from a Proxmox VE Shutdown VM

Before You Begin
When you are ready to remove the USB Flash drive, select **Un-Mount** from the Maintenance page.

About This Task
Follow these steps to remove the flash drive.

Note
The Virtual Appliance can be in service when the USB flash drive is assigned to it. Within a few seconds of the USB flash drive being assigned to it, the virtual appliance will detect the flash drive and mount it for use.

Procedure

1. Log in to the Proxmox GUI.
2. In the left pane, select the VM from the KVM server host name.
3. Select **Hardware**.
4. Select the corresponding USB device in the device list.
5. Select **Remove**.
6. Select **Yes** to confirm.

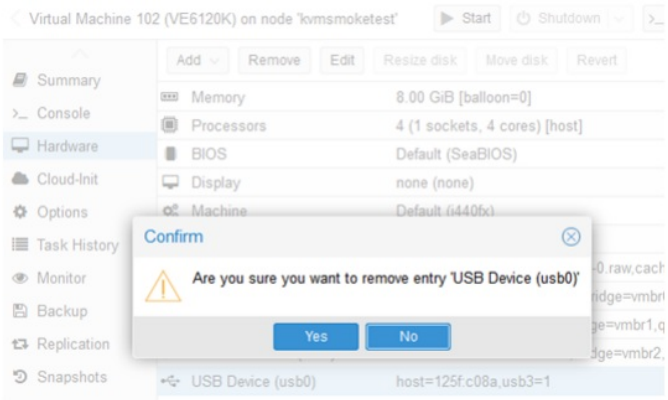


Figure 22: Confirm USB Device Removal

The USB flash drive can be removed from the host.

Shut Down and Restart a Virtual Machine Using the Graphical User Interface (GUI)

About This Task
To shut down and restart a virtual machine using the GUI:

Procedure

1. Navigate to **Administration** > **System** > **Maintenance**.
2. Select **Halt System (SHUTDOWN)**.

   The machine shuts down.
3. To restart the machine, select **Restart System (REBOOT)**.

   The machine restarts.

Remove the Flash Drive from a Proxmox VE Operational VM

Before You Begin

When you are ready to remove the USB Flash drive, select **Un-Mount** from the Maintenance page.

About This Task

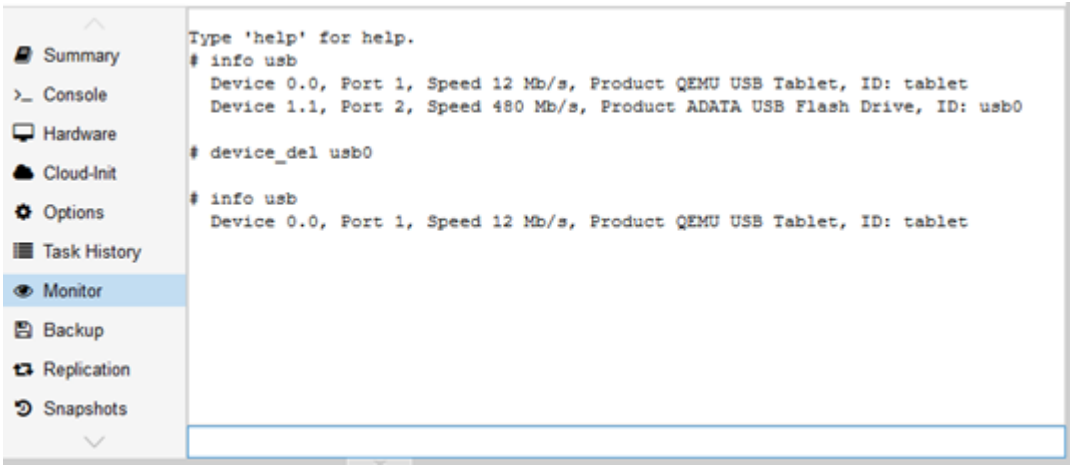
Follow these steps to remove the flash drive.

Note

The Virtual Appliance can be in service when the USB flash drive is assigned to it. Within a few seconds of the USB flash drive being assigned to it, the virtual appliance will detect the flash drive and mount it for use.

Procedure

1. Log in to the Proxmox GUI.
2. In the left pane, select the VM from the KVM server host name.
3. Select **Monitor**.
4. In the CLI, type **`info usb`** to display the list of attached USB devices.



5. Type **`device_del usb0`**, where usb0 is the ID of the device that needs to be removed.

   The USB flash drive can be removed from the host.

Generate and Install the Activation Package

How to generate and install an Activation Package.

About This Task

All customers must generate and install an Activation Package for ExtremeCloud IQ Controller. Regardless of whether you obtain a new license or upgrade to ExtremeCloud IQ Controller. Take the following steps to generate and install the Activation Package:

Procedure

1. Log in to ExtremeCloud IQ Controller.
2. Go to **Administration** > **License** to obtain the system **Locking ID**.
3. Log into the Extreme Support Portal.
4. Go to **Assets** > **Licenses Home** and select the ExtremeCloud IQ Controller Voucher ID line item from the list.
5. On the **Voucher Details** page, select **Generate Activation Key**.
6. Provide the Locking ID for the ExtremeCloud IQ Controller that will be activated.
7. Check the box to accept **Terms and Conditions** and select **Submit**.
8. The Activation package is generated, and the **Save As** dialogue displays.
9. Download the Activation Package to your local machine.



Note
The Activation Package *file name* includes the Locking ID for the specific ExtremeCloud IQ Controller.

Install the Activation Package

About This Task
Stage your ExtremeCloud IQ Controller instance. Install the Activation Package to activate ExtremeCloud IQ Controller:

Procedure

1. Return to the ExtremeCloud IQ Controller instance from where you obtained the Locking ID.
2. Go to **Administration** > **License**.
3. Select the plus sign next to the **Activation License** field.
4. Drag the Activation Package to the **Upload License** dialog to install the Activation Package.

Subscription License

ExtremeCloud IQ Controller is available for subscription licensing only, leveraging a single subscription SKU with ExtremeCloud IQ. The number of licenses corresponds to the number of managed access points. For more information, see the "Product Subscription License" section of the ExtremeCloud IQ Controller User Guide.

Related Links

Generate and Install the Activation Package on page 42

Shut Down and Restart a Virtual Machine

About This Task

The following task will outline the various ways through which you can shut down and reboot a virtual machine.

For information on how to access the Basic Configuration Wizard, see Access the Virtual Appliance Console on page 27.

To shut down and reboot the virtual machine using the Command Line Interface (CLI) in the Basic Configuration Wizard:

Procedure

1. Type **`shutdown halt`** and press **Enter** in the Basic Configuration Wizard.

   The virtual machine shuts down.
2. To reboot the virtual machine, type **`shutdown reboot`** and press **Enter**.

   The virtual machine restarts.

Shut Down and Restart a Virtual Machine Using the Graphical User Interface (GUI)

About This Task

To shut down and restart a virtual machine using the GUI:

Procedure

1. Navigate to **Administration** > **System** > **Maintenance**.
2. Select **Halt System (SHUTDOWN)**.

   The machine shuts down.
3. To restart the machine, select **Restart System (REBOOT)**.

   The machine restarts.

Shut Down and Restart a Virtual Machine on Proxmox VE server

About This Task

You can shut down and restart a virtual machine through the Proxmox VE server.



Note

QEMU Guest Agent has to be enabled per Virtual Machine for this to function as expected.

Procedure

1. Log in to the Proxmox GUI.
2. In the left pane, select the VM from the KVM server host name.
3. To shut down the virtual machine, select **Shutdown** in the menu.

4. To restart the virtual machine, select **Reboot** in the menu.

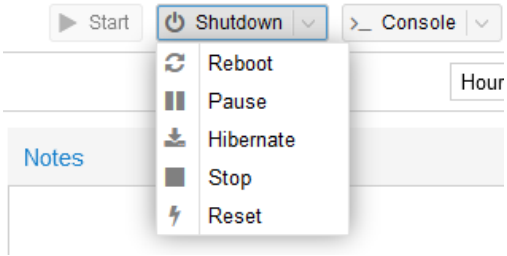


Figure 23: Proxmox GUI

Configure Bridges for the Virtual Appliance

Create a New Bridge on the KVM Server - Generic Procedure on page 45
Create a New Bridge on the KVM Server - Proxmox VE Procedure on page 45
Configure the Bridge for Jumbo Frames Support - Generic Procedure on page 46
Configure the Bridge for Jumbo Frames Support - Proxmox VE Procedure on page 46

The Virtual Appliance has some specific requirements on the bridges to which its data plane ports are connected. The following section explains how to create a bridge on a host that satisfies these requirements.

Create a New Bridge on the KVM Server - Generic Procedure

About This Task

This is an optional step since it is possible to reconfigure an existing bridge on the host. However, using separate bridge for the data plane traffic helps to isolate that traffic from other virtual devices.

To create a new bridge using the generic procedure:

Procedure

Create a Linux bridge attached to the desired network device.

Example:

```
iface ens3f0 inet manual

         auto vmbr1
         iface vmbr1 inet manual
               bridge-ports ens3f0
               bridge-stp off
               bridge-fd 0
```

Create a New Bridge on the KVM Server - Proxmox VE Procedure

About This Task

To create a new bridge using the Proxmox VE procedure:

Procedure

1. Log into the Proxmox GUI.
2. In the left pane, select the KVM server host name.
3. Select **System** > **Network**
4. Select **Create**.

5. Select **Linux Bridge** from the drop-down list.

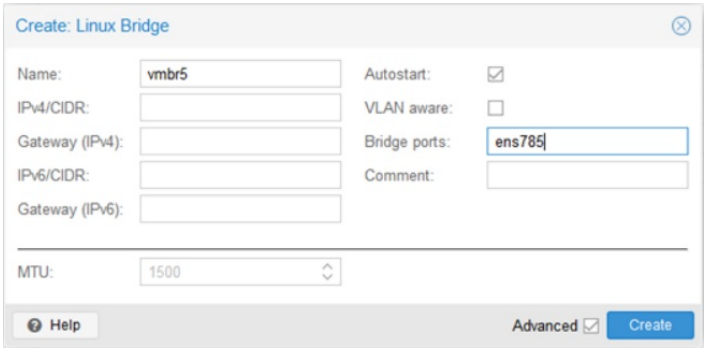


Figure 24: Create Linux Bridge Window

6. Set a Linux bridge name.
7. Set a bridge ports name that matches the network device name of the bridge.
8. Select **Create**.

Configure the Bridge for Jumbo Frames Support - Generic Procedure

About This Task

The jumbo frames feature enables the configuration of physical Maximum Transmission Unit (MTU) sizes up to 1800 bytes on the access point and appliance Ethernet data plane ports. The Admin port, all protocols, and interfaces continue to use the standard MTU size of 1500 bytes.

Enable Jumbo Frames to facilitate the transmission of MU data between the access point and the appliance, or between the access point and a bridge for VxLAN topologies, without incurring fragmentation.

To configure the bridge for jumbo frames support using the generic procedure:

Procedure

Set the MTU of the network devices and the data plane ports attached bridges to 1800.

Configure the Bridge for Jumbo Frames Support - Proxmox VE Procedure

About This Task

The jumbo frames feature enables the configuration of physical Maximum Transmission Unit (MTU) sizes up to 1800 bytes on the access point and appliance Ethernet data plane ports. The Admin port, all protocols, and interfaces continue to use the standard MTU size of 1500 bytes.

Enable Jumbo Frames to facilitate the transmission of MU data between the access point and the appliance, or between the access point and a bridge for VxLAN topologies, without incurring fragmentation.

To configure the bridge for jumbo frames support using the Proxmox VE procedure:

Procedure

1. In the left pane, select the VM from the KVM server host name.
2. Select **System** > **Network**.
3. Select the network device that must be configured.
4. Select **Edit**.

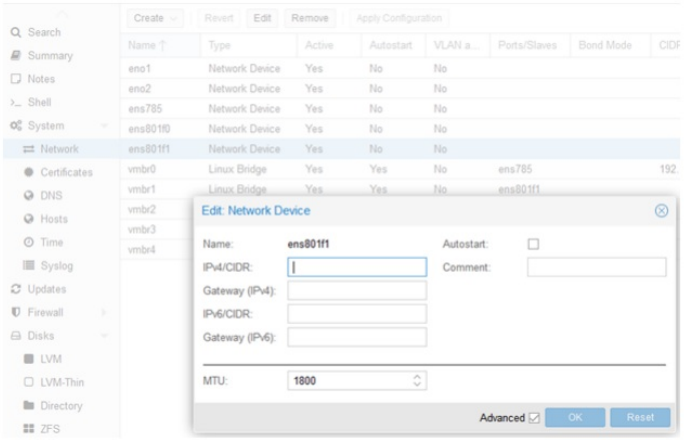


Figure 25: Network Device Edit Window

5. Set the MTU value to 1800.
6. Select **OK**.
7. Select the Linux bridge attached to the corresponding network device.
8. Select **Edit**.

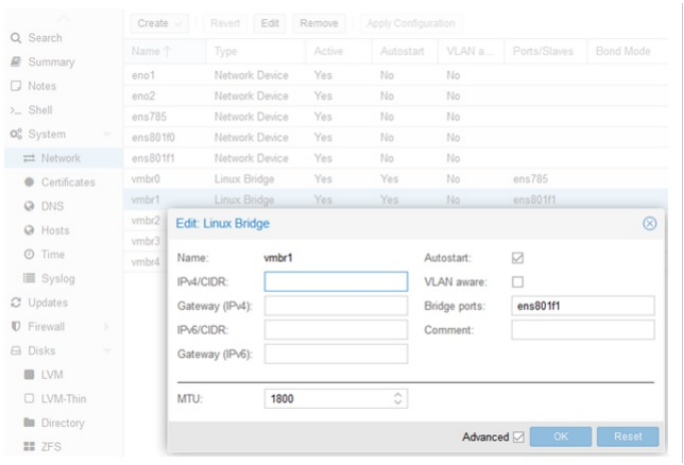
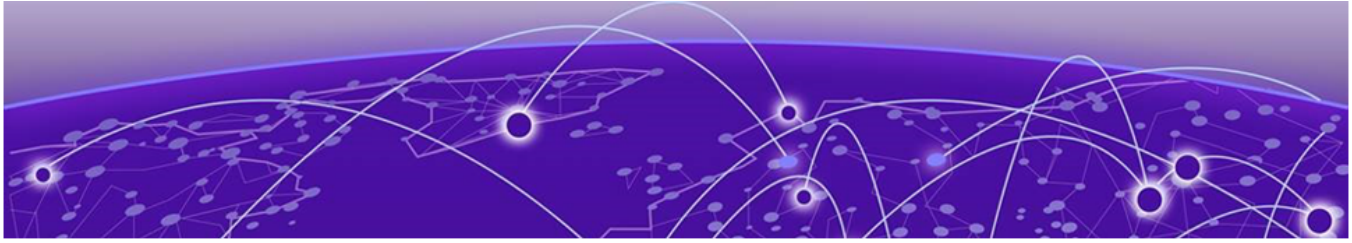


Figure 26: Linux Bridge Edit Window

9. Set the MTU value to 1800.
10. Select **OK**.



Index

A

announcements 9, 10

B

backup
    backup config 34
    backup schedule 34
    perform a backup 34
    store backup file 34
bridge configuration 46

C

conventions
    notice icons 7
    text 7
copy backup 34

D

documentation
    feedback 10
    location 8, 9

F

feedback 10

J

jumbo frames
    Proxmox VE 46
jumbo frames support 46

K

KVM bridge generic procedure 45
KVM bridge Proxmox VE procedure 45
KVM server 45

L

licensing
    Activation Package 42

N

new bridge 45
notices 7

P

product announcements 9, 10
Proxmox VE virtual appliance deployment 17

R

restart using GUI 40

S

Subscription License 42
support
    technical support 9, 10

T

technical support
    contacting 9, 10

U

upgrade software 32
upload method 34

V

VE6120K connectivity requirements 13
VE6125K connectivity requirements 13
virtual machine
    reboot 43
    restart 43
    shut down 43

W

warnings 7