ExtremeMobility™

VE6120/VE6125 Virtual Appliances Installation Guide VMware® Platform

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, please see:
www.extremenetworks.com/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:
www.extremenetworks.com/support/policies/software-licensing

Table of Contents

Preface

This section discusses the conventions used in this guide, ways to provide feedback, additional help, and other Extreme Networks® publications.

Text Conventions

The following tables list text conventions that are used throughout this guide.

Table 1: Notice Icons

Icon	Notice Type	Alerts you to...
	General Notice	Helpful tips and notices for using the product.
	Note	Important features or instructions.
	Caution	Risk of personal injury, system damage, or loss of data.
	Warning	Risk of severe personal injury.
New!	New Content	Displayed next to new content. This is searchable text within the PDF.

Table 2: Text Conventions

Convention	Description
`Screen displays`	This typeface indicates command syntax, or represents information as it appears 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 with brackets, such as **[Return]** 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.

Providing Feedback to Us

Quality is our first concern at Extreme Networks, and we have made every effort to ensure the accuracy and completeness of this document. We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:
- Content errors or confusing or conflicting information.

- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team, you can do so in two ways:

- Use our short online feedback form at https://www.extremenetworks.com/documentation-feedback/.
- Email us at documentation@extremenetworks.com.

Please provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

Getting Help

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: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. 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 and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) 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

Subscribing to Service Notifications

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

1 Go to www.extremenetworks.com/support/service-notification-form.
2 Complete the form with your information (all fields are required).

3 Select the products for which you would like to receive notifications.

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

4 Click **Submit**.

Documentation and Training

To find Extreme Networks product guides, visit our documentation pages at:

Current Product Documentation	www.extremenetworks.com/documentation/
Archived Documentation (for earlier versions and legacy products)	www.extremenetworks.com/support/documentation-archives/
Release Notes	www.extremenetworks.com/support/release-notes
Hardware/Software Compatibility Matrices	https://www.extremenetworks.com/support/compatibility-matrices/
White papers, data sheets, case studies, and other product resources	https://www.extremenetworks.com/resources/

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For more information, visit www.extremenetworks.com/education/.

1 Overview

The guide describes how to configure and deploy the ExtremeCloud™ Appliance VE6120 and VE6125 Virtual Appliances. This guide is a reference for system administrators who install and manage the VE6120 and VE6125 Virtual Appliances.

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

2 Virtual Appliance Deployment

Deployment Requirements
Connectivity Requirements
Downloading a VE6120/VE6125 Image

This section provides an overview of the requirements for the ExtremeCloud™ ApplianceVirtual Appliances VE6120 and VE6125 deployments. It explains how to install the appliances on a VMware® vSphere™ server (ESXi™) and how to run the initial configuration wizard.

Deployment Requirements

The VE6120/VE6125 are packaged in the .ova file format defined by VMware. The appliances must be deployed on a VMware ESXi host running vSphere.

> **Note**
> VE6120 and VE6125 use separate .ova files. You cannot upgrade from VE6120 to VE6125.

> **Note**
> The VE6125 requires an enterprise VMware license to launch and run the virtual machine.

The minimum supported version of vSphere for VE6120 is 5.1 and for VE6125 is 5.5.

> **Note**
> You only need to install the .ova file when you first install the appliance. All subsequent upgrades can be performed using the standard controller upgrade procedure to apply a .dle file to the VE6120 appliance and .rse file for the VE6125 appliance.

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

If all three interfaces are used, it is recommended to connect them to separate virtual switches (vSwitches) in the host server.

Configuration Options:
* Small reflects the default configuration for VE6120.
* XLarge is the default and only configuration available for VE6125.

Table 3: Virtual ExtremeCloud Appliances (VE6120 and VE6125)

Extreme Application		VE6120		VE6125
	Small	Medium	Large	X-Large
Total APs managed in Standalone mode	50	250	500	2000

Table 3: Virtual ExtremeCloud Appliances (VE6120 and VE6125) (continued)

Extreme Application	VE6120			VE6125
Additional APs supported in high-availability mode	50	250	500	2000
Total managed APs per Appliance Pair	100	500	1000	4000
Total Switches managed per Appliance	50/100	100/200	200/400	200/400
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 (4 distinct physical cores or 2 cores with hyper-threading)	6	8	32 (physical or hyper-threading cores)
RAM (GB)	8	16	24	32
Hard Disk (GB)	80	80	80	512
2x1Gbps Host (Open/Secure Mbps)	1,870/1,870	1,870/1,870	1,870/1,870	—
2x10 Gbps Host (Open/Secure Mbps)	10,800/5,100	10,800/5,100	10,800/5,100	—

- Consult VMWare ESXi 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.
- Follow VMWare minimum installation requirements. 10 Gbps host recommended for best results. VE6120 supports VMware ESXi 5.1 or higher. VE6125 supports VMware ESXi 5.5 or higher.
- A VMware Enterprise license is required for the VE6125.

Connectivity Requirements

The appliances have one management interface (Admin) and two data plane interfaces (Port1, Port2). If all three interfaces are used, it is recommended to connect them to separate virtual switches (vSwitches) in the ESXi host.

The data plane interfaces have additional requirements on the vSwitches to which they connect:
- The vSwitch must be configured to accept promiscuous mode connections.
- The vSwitch must be configured to accept any VLAN tag traffic and forward it without changing or removing the VLAN tags.

Although configuring the necessary vSwitches does not have to be done before installing the appliance, the installation process will be simpler if it is.

See Configuring vSwitches for the Virtual Appliance for instructions on how to create and configure vSwitches that can be used by the Virtual Appliance's data plane ports.

Downloading a VE6120/VE6125 Image

Download the VE6120/VE6125 software image to your local machine where you manage the vSphere.

1 Access the VE6120/VE6125 download page at https://extremeportal.force.com/.
2 Download the image from **Downloads > Downloads Home** tab.

    1 Log into the **Downloads Home** using your Extreme Portal login credentials.
    2 Type VE6120/VE6125 in the search tab and click the search icon. The image list is displayed.
    3 Download the **latest** VE6120/VE6125 Virtual Appliance Image.

Logging in to the vSphere Client

To login to the vSphere server:

1 Launch a web browser and enter the vSphere address to access the vSphere application.
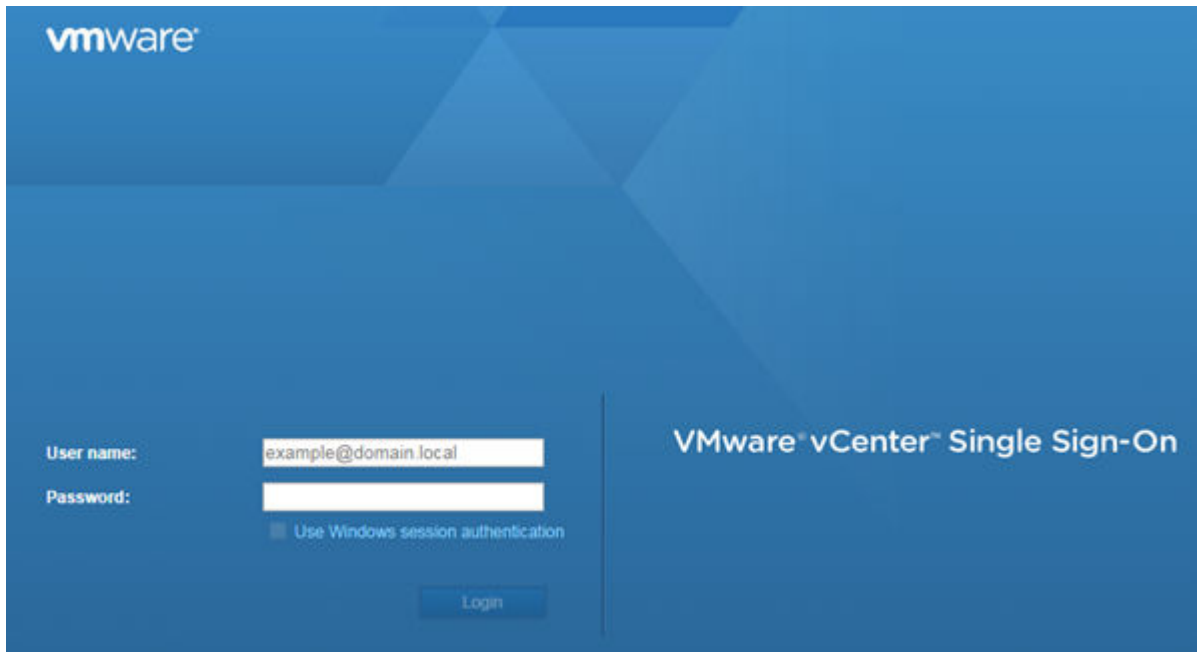
    The Web Client login screen displays.

Figure 1: VMware vSphere Web Client Login Screen

2 On the VMware vSphere Web Client login screen:
   • Enter the User name and Password of an account that has full administrative access to the vSphere (ESXi) server.
   • Click **Login**.

Installing and Deploying the Virtual Appliance Image

To install the Virtual Appliance image:

1   From the **Navigator** tab in the vSphere Web Client, right-click the host machine and select **Deploy OVF Template**.
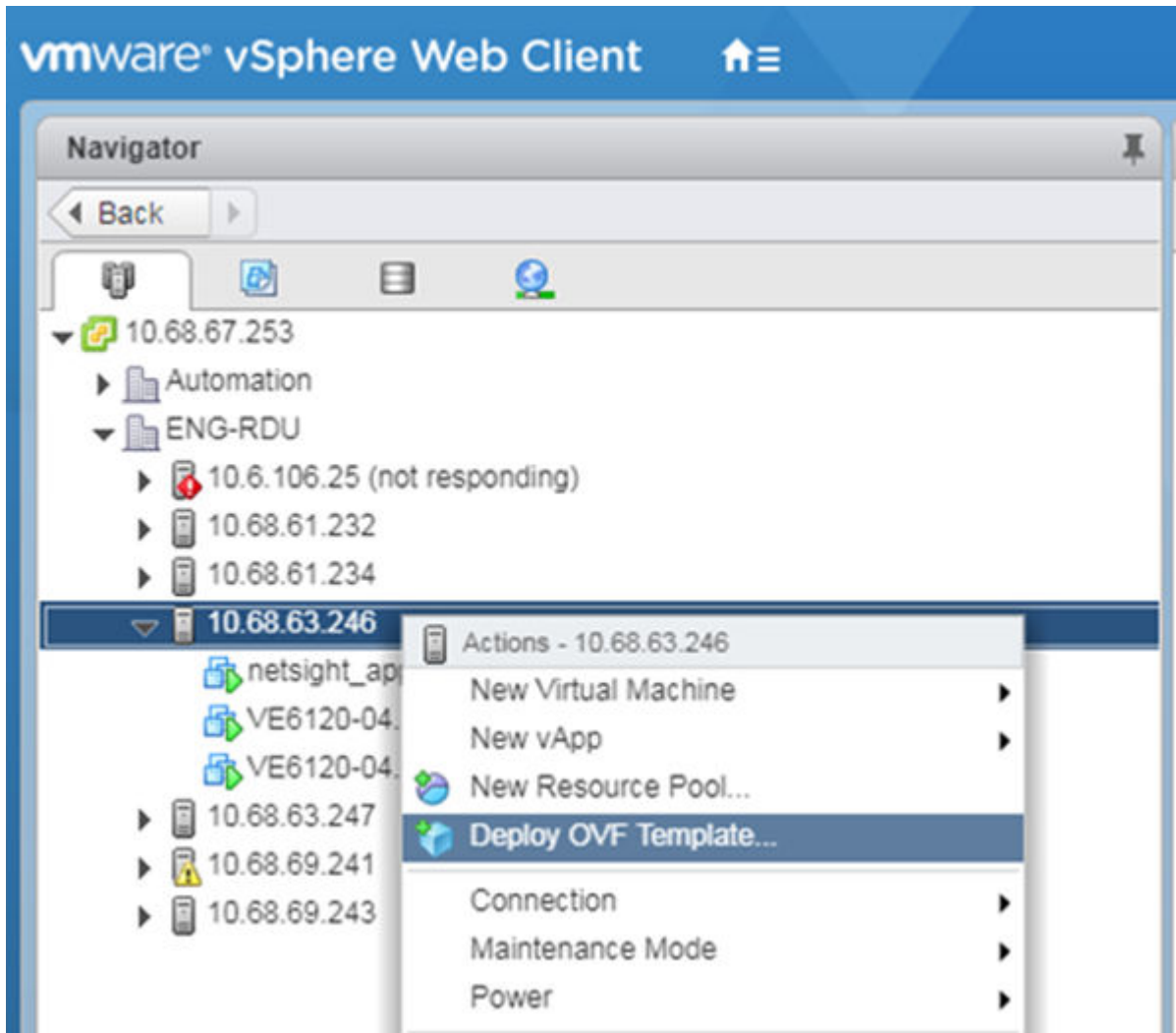

Figure 2: Deploy OVF Template option

> **Note**
> Even though the VE6120 is distributed in the .ova file format, it is compatible with the menu option of alternate .ovf format.

2   On the **Deploy OVF Template** window:

- Click **Browse** to select the VE6120 .ova file that you downloaded in the Downloading a VE6120/VE6125 Image on page 10 section, and click **Next**. The **Name and Location** screen is displayed.
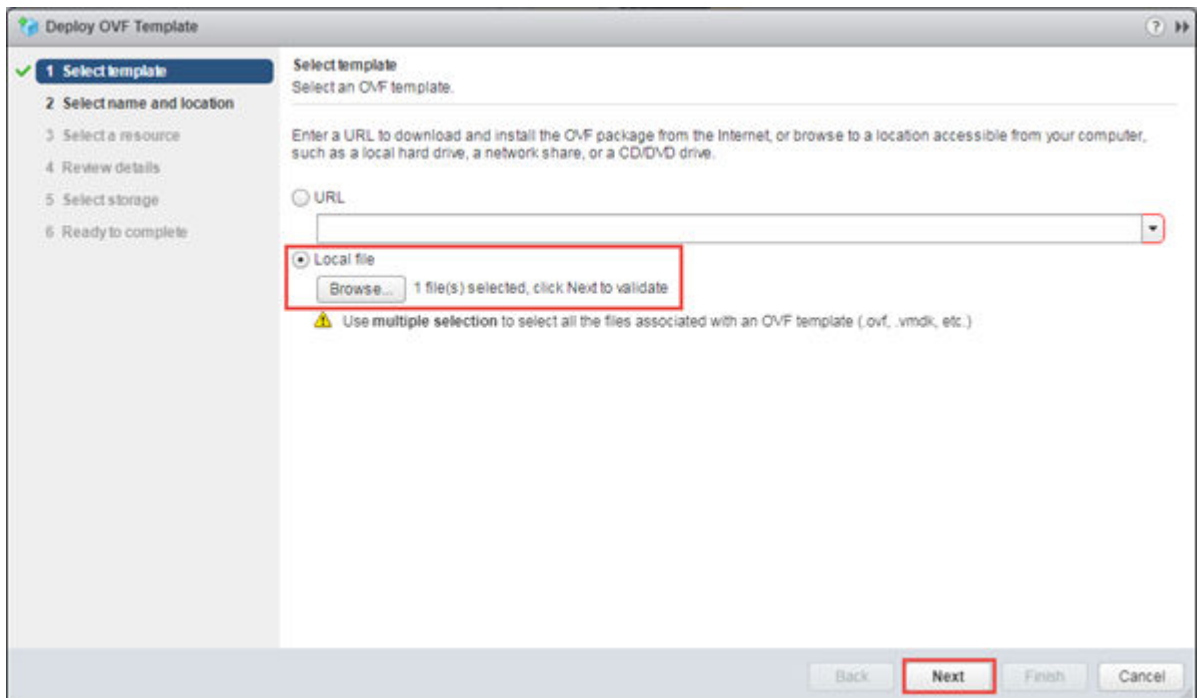

Figure 3: Deploy OVF Template Window

Or

- You can select a source URL to download and install the OVA file.

3   On the **Name and Location** screen, enter a name for the VE6120, select a datacenter folder, and click **Next**. **Select a resource** screen is displayed.

> **Note**
> The name you enter will be used in the vSphere client's inventory list. It does not have to be the same name as the hostname of the VE6120/VE6125 appliance.
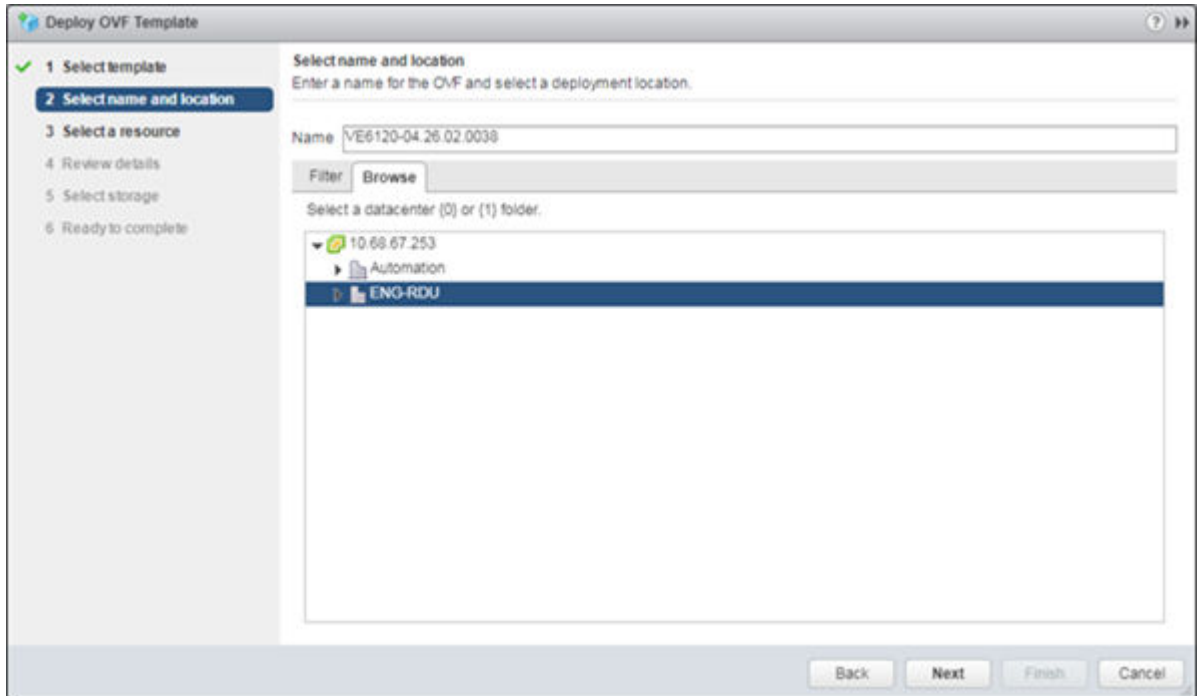

Figure 4: Name and Location screen

4   On the **Select a resource** screen, select a host server, and then click **Next**. The **Review details** screen is displayed.
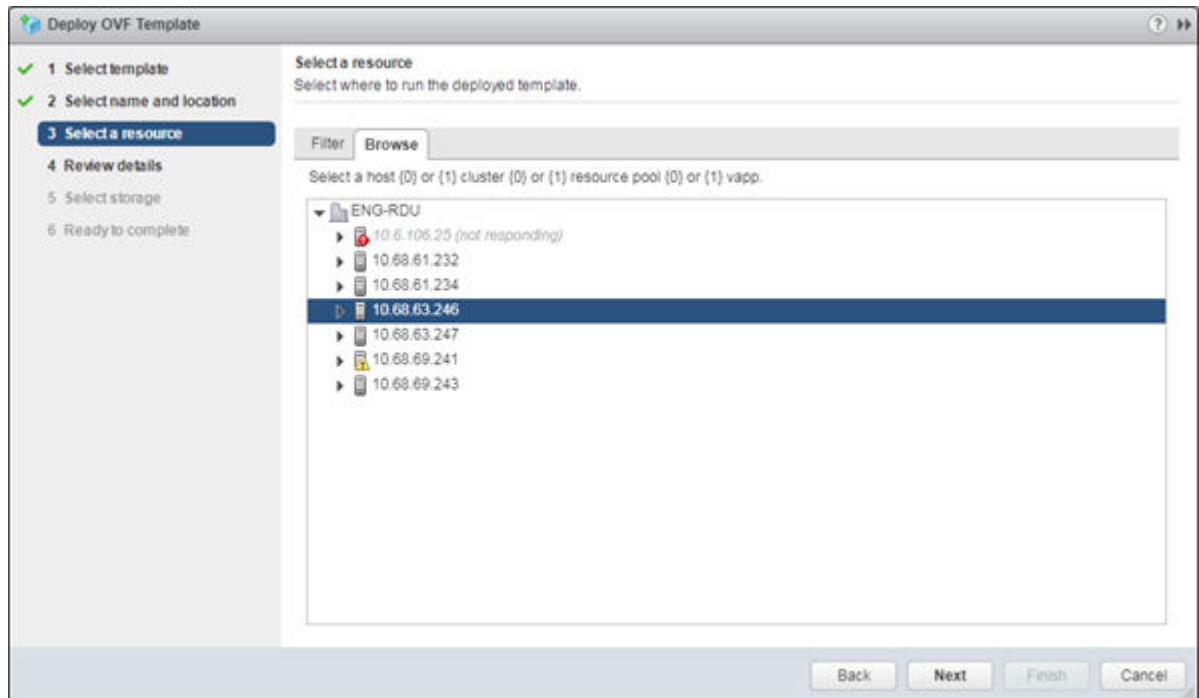

Figure 5: Select a resource screen

5   On the **Review details** screen, review the information and click **Next**.**Select storage** screen is displayed.

> ![Note icon] **Note**
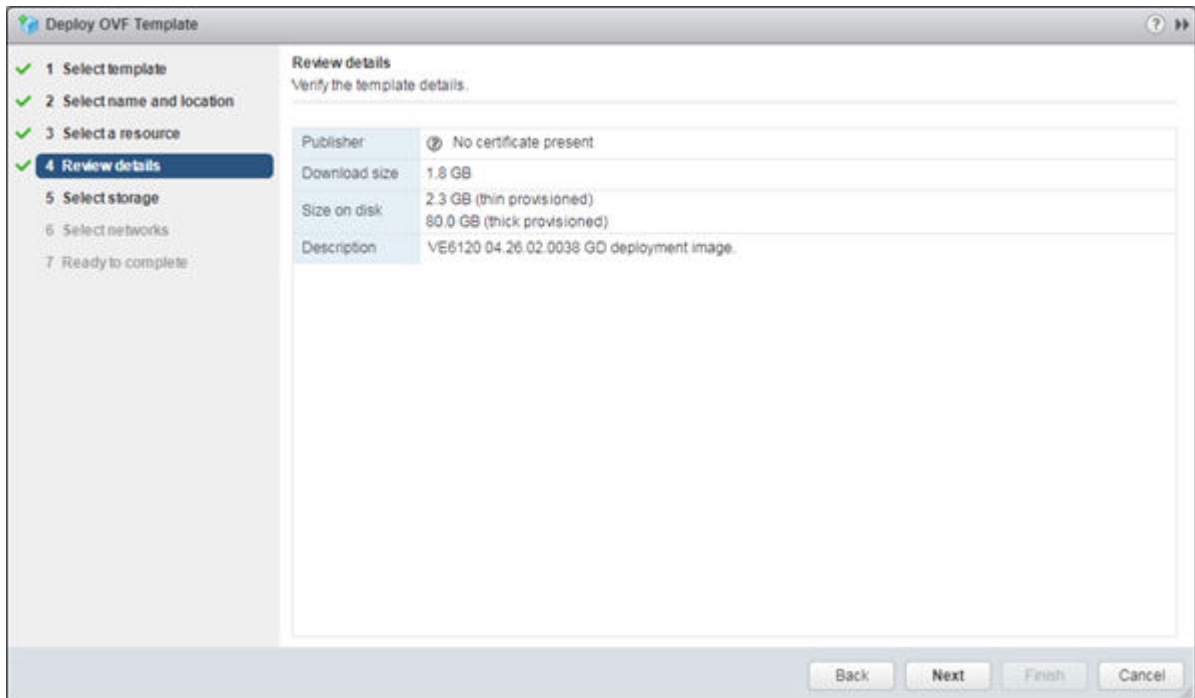> You can click **Back** to modify any of the previous settings.

Figure 6: Review details screen

6   On the **Select storage** screen:

1   Select virtual disk format as **Thick provision**. This is the default virtual disk format.

> ![Note icon] **Note**
> Thick provision format allocates storage immediately. For more information on disk storage, see Deployment Requirements on page 8.

2   Select your destination storage.

3   Click **Next**.

The **Select networks** screen is displayed.

7   On the **Select networks** screen, map the virtual appliance ports to the virtual networks that are deployed on the host server. For each **Source Network**, select a corresponding **Destination Network**.

Table 4: Network Selection

Source Network	Destination Network/ Description
VM Network	MGMT-63/Management port
Port 2	Internal 1
Port 1	450-P8

Click **Next**. The **Ready to complete** screen is displayed.

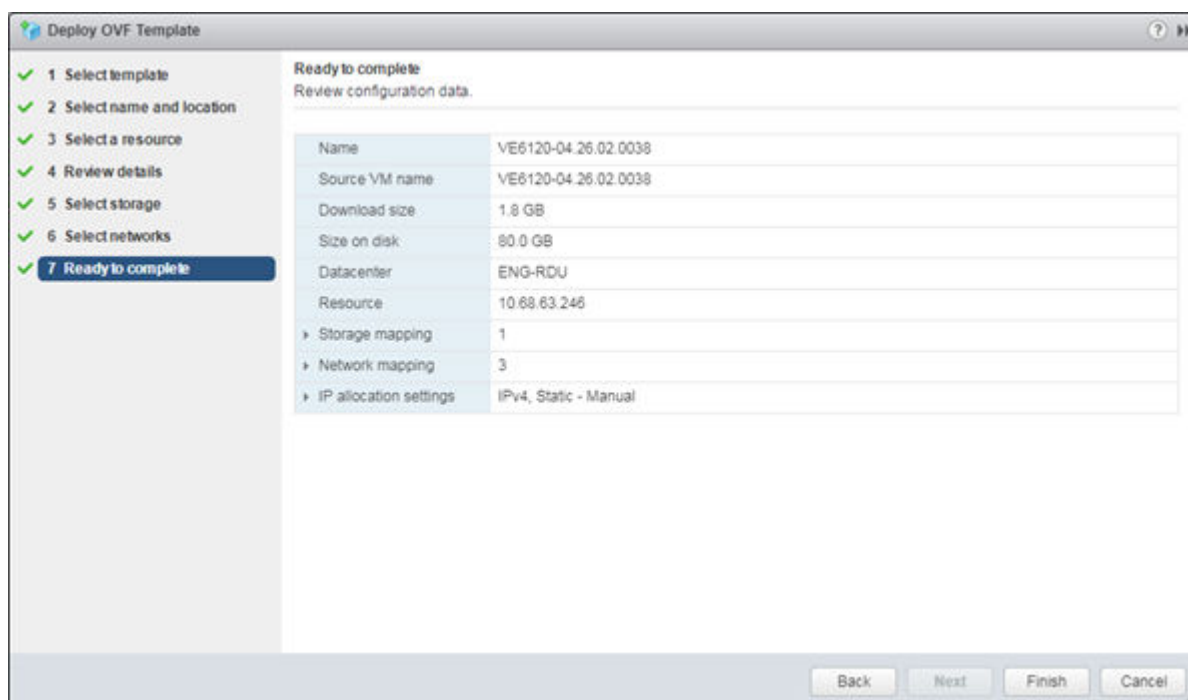8   Review your configuration data in the **Ready to complete** screen, click **Finish** to finish your setup.

Figure 7: Ready to Complete screen

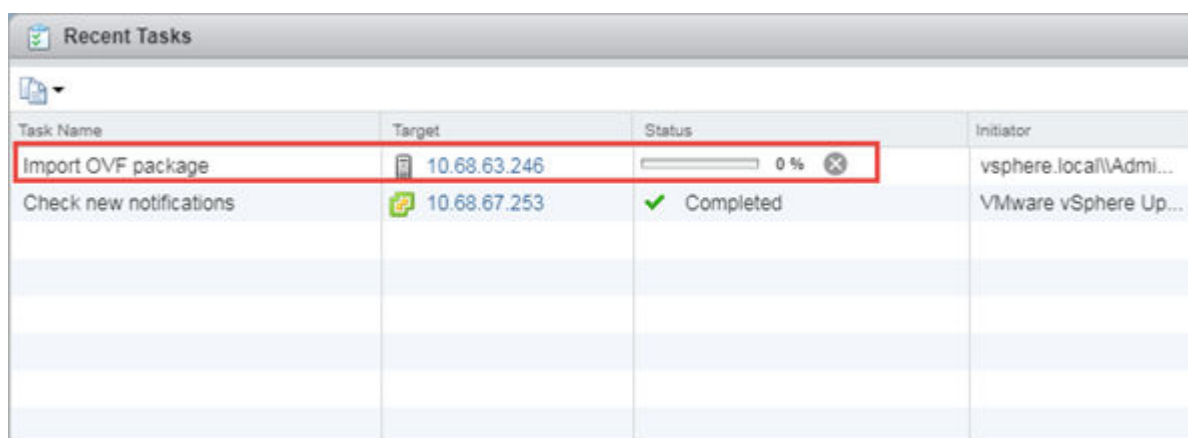A progress bar is displayed in the **Recent Tasks** section.

Figure 8: Progress bar

When the deployment has completed successfully, click **Close**.

3 Virtual Appliance Configuration

Accessing the Virtual Appliance Console
Configuring the VE6120/VE6125 using the Basic Configuration Wizard
Setting up the VE6120/VE6125 appliance using the Basic Configuration Wizard
Upgrading the VE6120/VE6125 Software
Setting Up the Virtual Appliance to Accept USB Flash Drives
Activating the ExtremeCloud Appliance

After the Virtual Appliance has been deployed on a VMware ESXi server using the instructions in Virtual Appliance Deployment on page 8 you are ready to perform initial server configuration.

Accessing the Virtual Appliance Console

To log in to the Virtual Appliance and perform the initial configuration, access the vSphere client's console window as follows:

1 Launch a web browser and enter vSphere address to open the vSphere web client application.

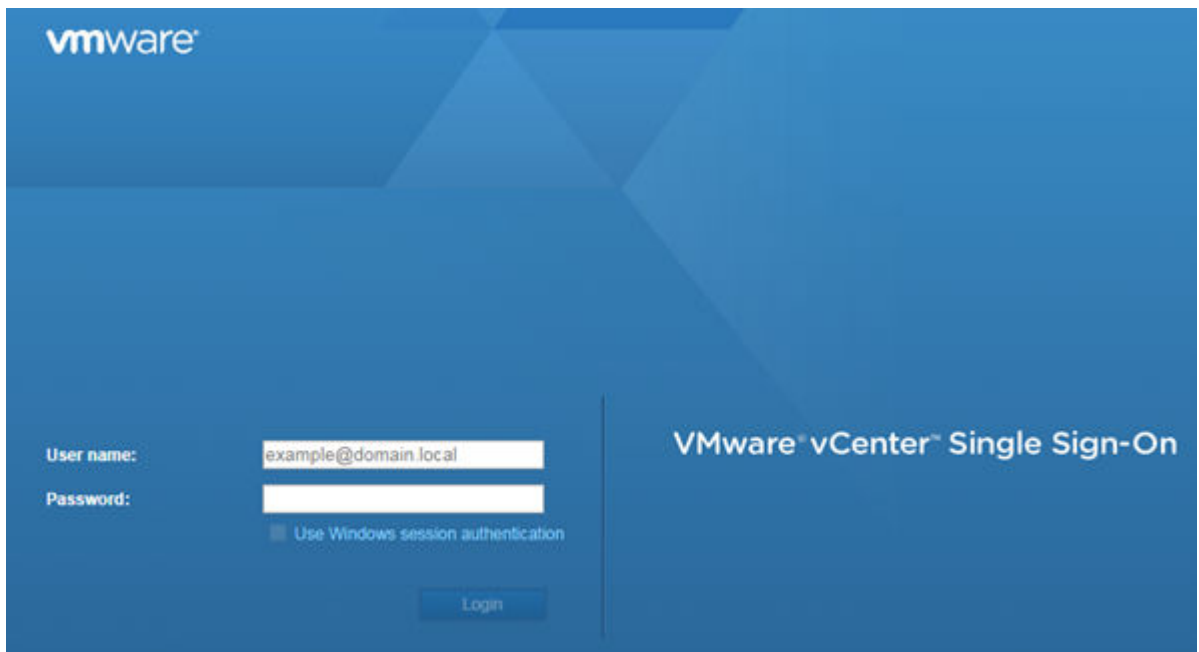The **VMware vSphere Web Client** login screen is displayed.

Figure 9: VMware vSphere Web Client Login Screen

2 On the VMware vSphere Web Client login screen:

- Enter the User name and Password of an account that has full administrative access to the vSphere (ESXi) server.
- Click **Login**.

3 On the **vSphere Web Client** screen, in the left **Navigator** pane, expand the host mode, right-click the **Virtual Appliance** and select **Power** > **Power On**.
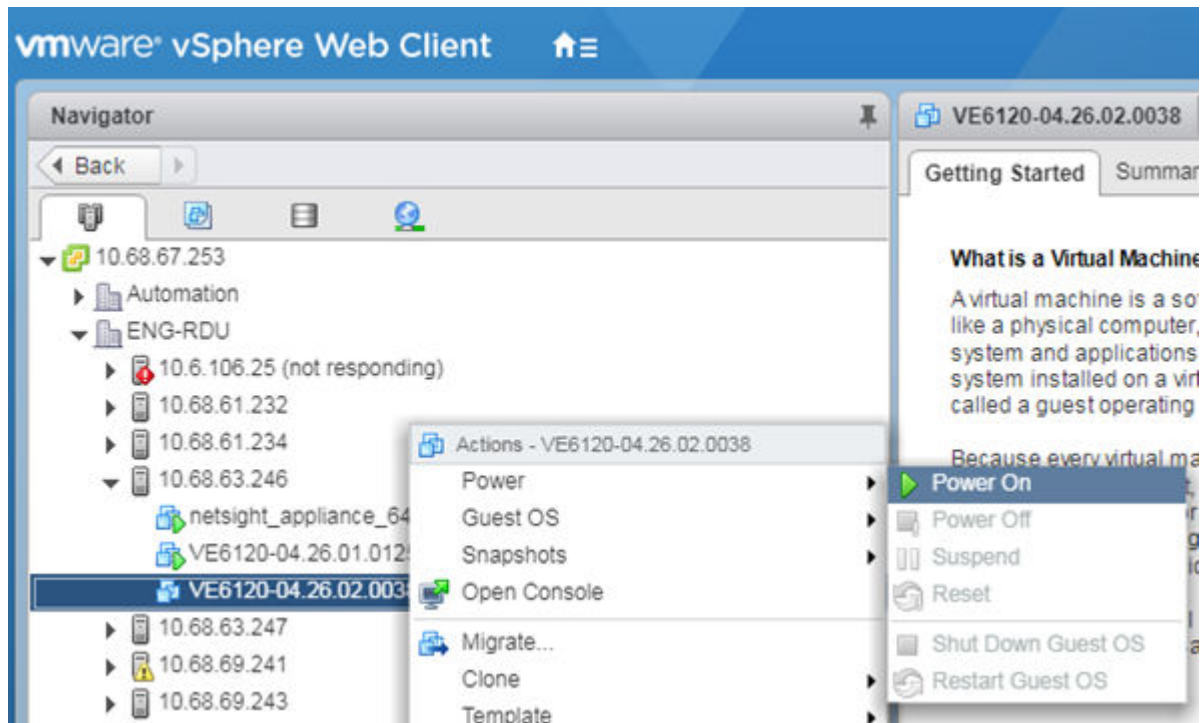

Figure 10: vSphere Web Client Power On option

> **Note**
>
> If the **Power On** option is greyed out, press the [icon] icon on the **vSphere Web Client** tool bar.

The Green icon indicates that the virtual appliance is powered on.

4   After the Virtual Appliance has been started and completes its boot process, right-click the
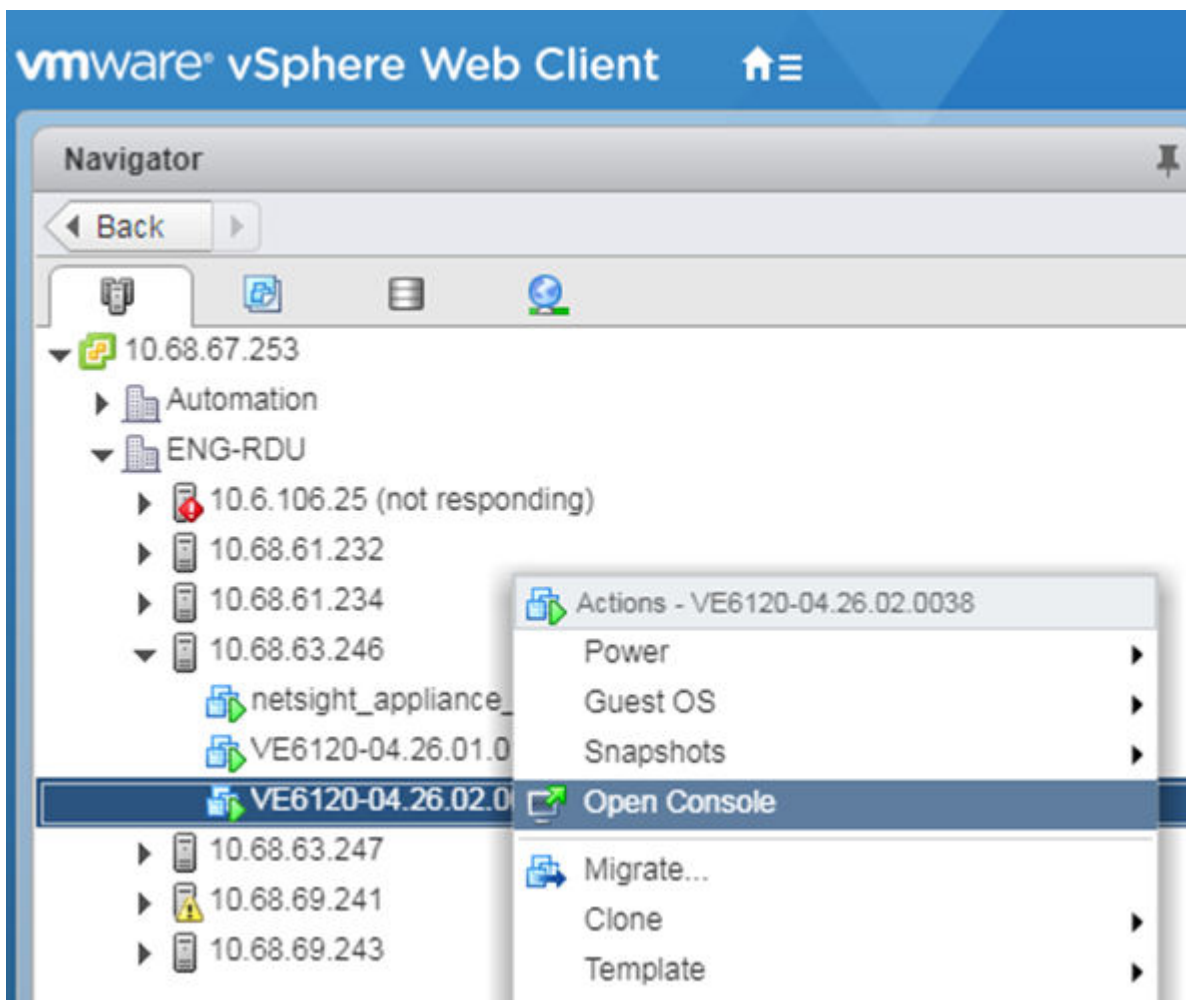   appliance name, and from the drop-down menu, click **Open Console**.

Figure 11: Open Console option

The VE6120 Command Line Interface (CLI) opens in a new window.

5   Enter your login credentials.

> **Note**
> Click inside the console window once or twice to make the window interactive. If the prompt is not visible, press **[Enter]**.

- For **User Name**, enter admin.
- For **Password**, enter abc123.

You now are working in the VE6120's CLI.

Figure 12: VE6120's Command Line Interface (CLI)

Configuring the VE6120/VE6125 using the Basic Configuration Wizard

The ExtremeCloud Appliance software provides a Basic Configuration Wizard that can help administrators configure the minimum settings necessary to deploy a fully functioning VE6120/VE6125 appliance on a network.

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

The wizard is automatically launched when an administrator logs on to the VE6120/VE6125 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**.

For more information about using the Basic Configuration Wizard, see Setting up the VE6120/VE6125 appliance using the Basic Configuration Wizard on page 21.

Setting up the VE6120/VE6125 appliance using the Basic Configuration Wizard

After logging into the CLI of the VE6120/VE6125 Basic Configuration Wizard, you will be able to set it up using a set of **Yes** or **No** commands.

1   After logging into the CLI of VE6120/VE6125, you will be prompted to change the admin password. To begin the admin password setup, press **Enter**. The **Admin password Configuration** screen is displayed.

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

   b   Enter the new password for the admin account.

> **Note**
> The password must be between 8-24 characters.

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

   If the passwords match, the password gets accepted.

   d   Press **Enter** to accept the changes.

   The AP access password screen is displayed.

2   To reset the AP access password, type a new password in the CLI.

> **Note**
> The password must be between 5-30 alphanumeric characters and can include period, dash, underscore, and space.

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

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

Current Data Port Settings

Once 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,

1   In the **Current Data Port Settings**, you will determine the port settings. The default port is **Port1**. Click **Enter** to select **Port1**.

2   Set IP Address to the default value. The default value is `10.0.0.1`. Press **Enter**.

   The IP Address is selected.

3   Set Netmask to default value of `255.255.255.0`. Press **Enter**.

   The Netmask is set.

4   Press **Enter** to set the default VLAN. The tagged frames command is displayed.

5   Press **Enter** to keep the default tagged frames value to `No`.

6   To enable management on the interface, press **Enter** to select the default value, `Yes`.

7   To enable device registration, press **Enter** to select the default value, `yes`. The updated Data Port Interface settings is displayed.

8   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** screen.

Current Host Attributes

To set up the current host attributes,

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`.

   A note is displayed that the Admin port does not allow device registration.

4 Type the IP address in the following format `xx.xx.xx.xxx` 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.x.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 is displayed.

Current Global Default Gateway Settings

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

1 Type an IP address.

2 Press **Enter** to accept the changes.

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

Current Time Settings

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

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.

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. Press **Enter**.

6 You are prompted to enter a second NTP server and the default option is `y`. Type `n` and press **Enter**.

   NTP Client is enabled.

7 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** screen along with the menu.

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

Figure 13: Controller Post Installation Configuration Menu Screen

Table 5: 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.

Upgrading the VE6120/VE6125 Software

If you are not installing the **latest** ExtremeCloud Appliance release, you need to upgrade the software to the latest patch release.

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

2   Log in to the virtual appliance using the admin user and password that you configured in the Setting up the VE6120/VE6125 appliance using the Basic Configuration Wizard on page 21 section.
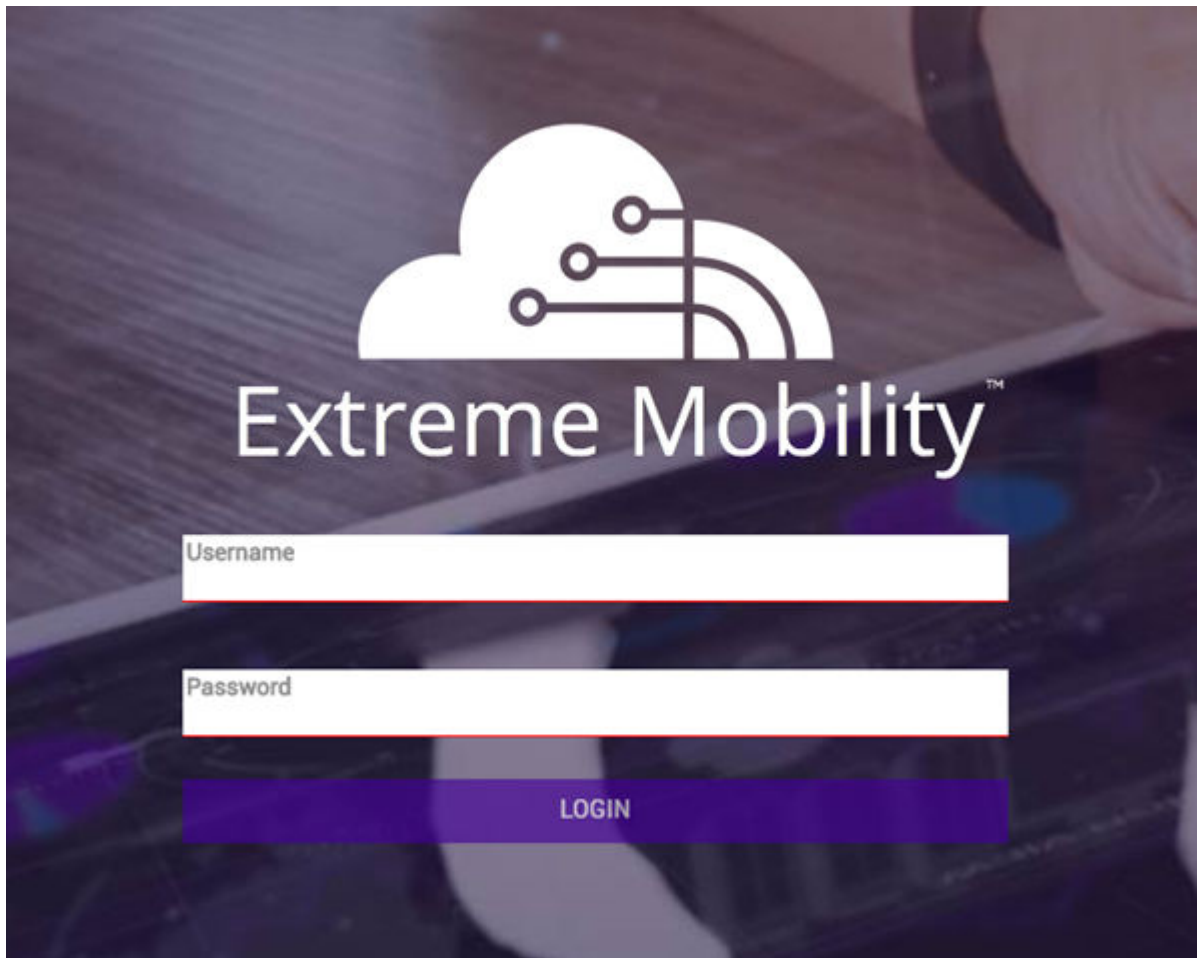

Figure 14: VE6120 Virtual Appliance Login Screen

3   Go to **Administration > System**. The System screen is displayed.
4   Select **Software Upgrade** tab. Navigate to the **Upgrade** section.

5   To add the image file, click the plus icon.

Figure 15: Upgrade section

The **Copy Upgrade Image** window is displayed.

6   From the Upload Method drop-down, select Local or FTP or SCP.

Option	Description
Local	If you select Local as your file upload method, drop the file into the **Select File or Drop File** area.
FTP or SCP	If you select FTP as your file upload method, enter the following details: • Service IP • Username • Password • Directory • Filename • Destination From the Destination drop-down, select Local or Flash.

7   Click **OK**.

The **Copy Upgrade Image** displays the progress of your image upload.

8   Once the image is uploaded, from the Backup System Image to field drop-down, select **Local**, or **Flash**, or **No Backup**.

> **Note**
> It is not recommended to select the **No Backup** option.

9   From the Upgrade drop-down select **Now** to upgrade your software or select **Schedule** to configure your upgrade schedule.

You have now successfully upgrade your software and the results are displayed in the **Upgrade Result** window.
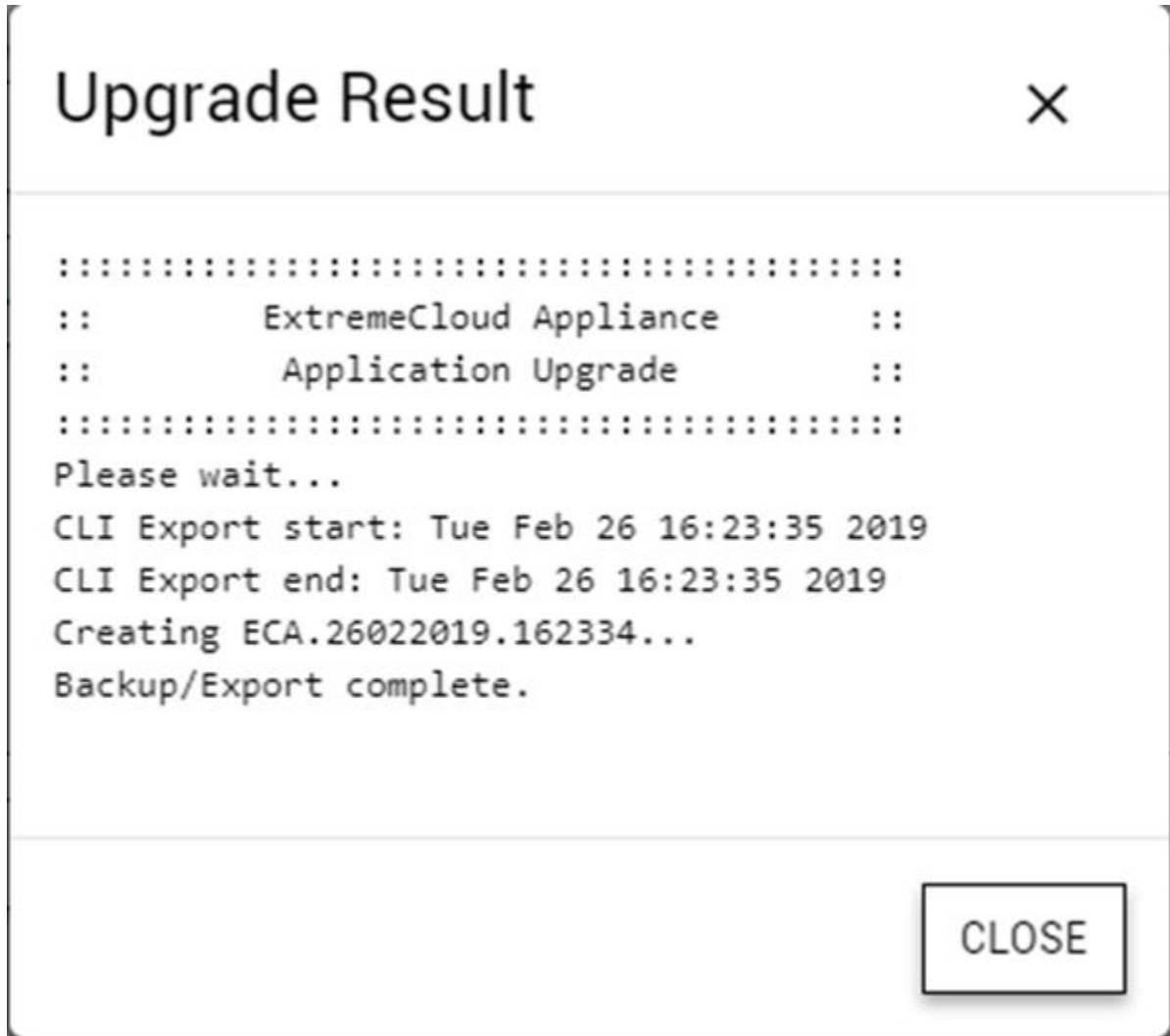
```
::::::::::::::::::::::::::::::::::::::::::::::::
::          ExtremeCloud Appliance        ::
::              Application Upgrade        ::
::::::::::::::::::::::::::::::::::::::::::::::::
Please wait...
CLI Export start: Tue Feb 26 16:23:35 2019
CLI Export end: Tue Feb 26 16:23:35 2019
Creating ECA.26022019.162334...
Backup/Export complete.
```

Figure 16: Upgrade Result window

For more information about the **Software Upgrade** options, see the ExtremeCloud Appliance User Guide.

Setting Up the Virtual Appliance to Accept USB Flash Drives

The Virtual Appliance has a (virtual) USB controller and 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 enable the Virtual Appliance to use a USB flash drive:

1   Format the flash drive to FAT32.

2   Insert the flash drive into a USB port on the host.

> **Note**
> The vSphere client application requires that a USB device be plugged in before it can be added to a virtual machine.

3   Log in to the vSphere client using an account that grants full administrative access to the VE6120.
4   From the list of guest operating systems (virtual machines), right-click on VE6120, and from the drop-down menu, select **Edit Settings**.
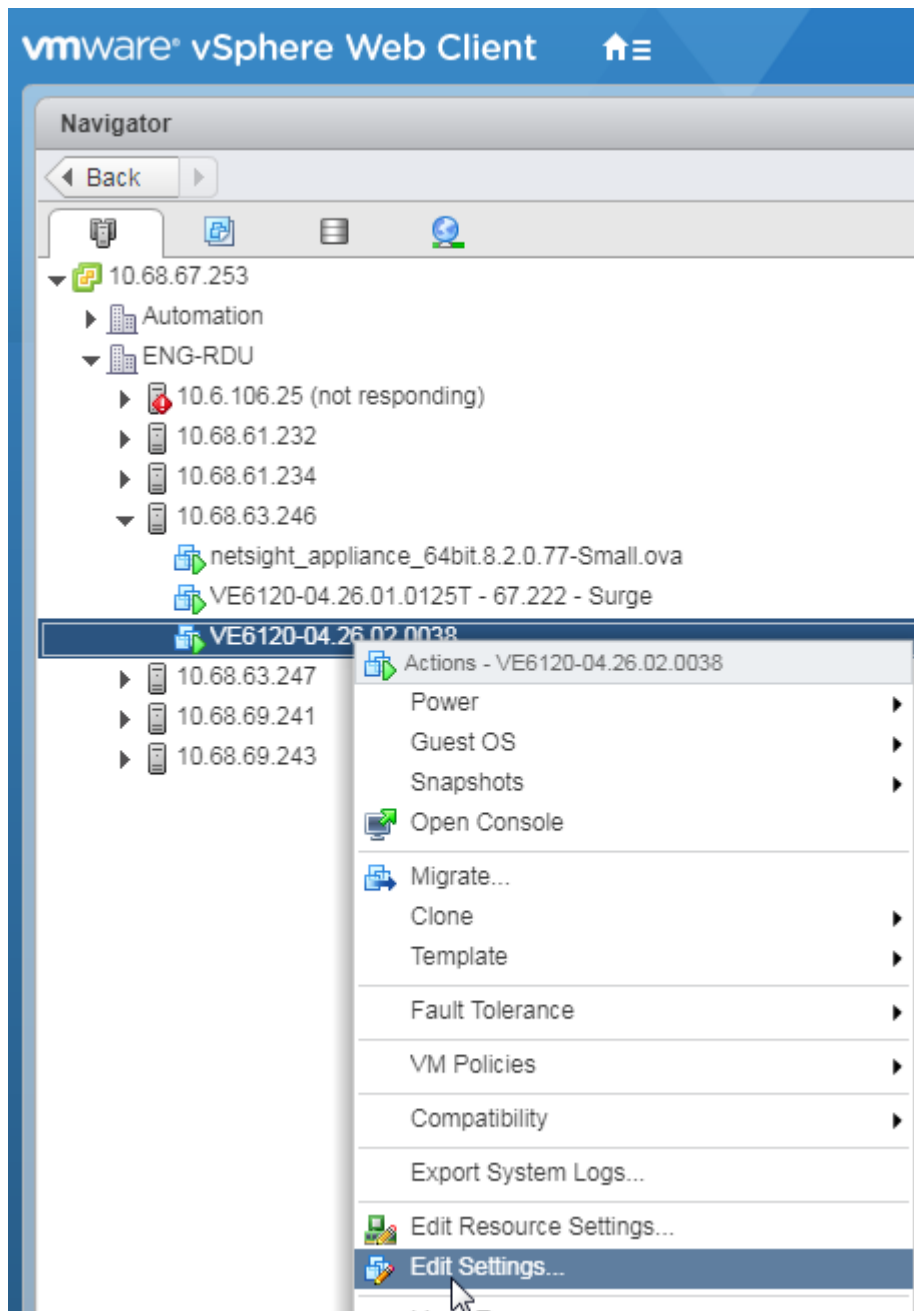

Figure 17: VE6120 Edit Settings Window

5   In the **Virtual Hardware** window, select **Host USB Device** from the drop-down, and click **Add**.
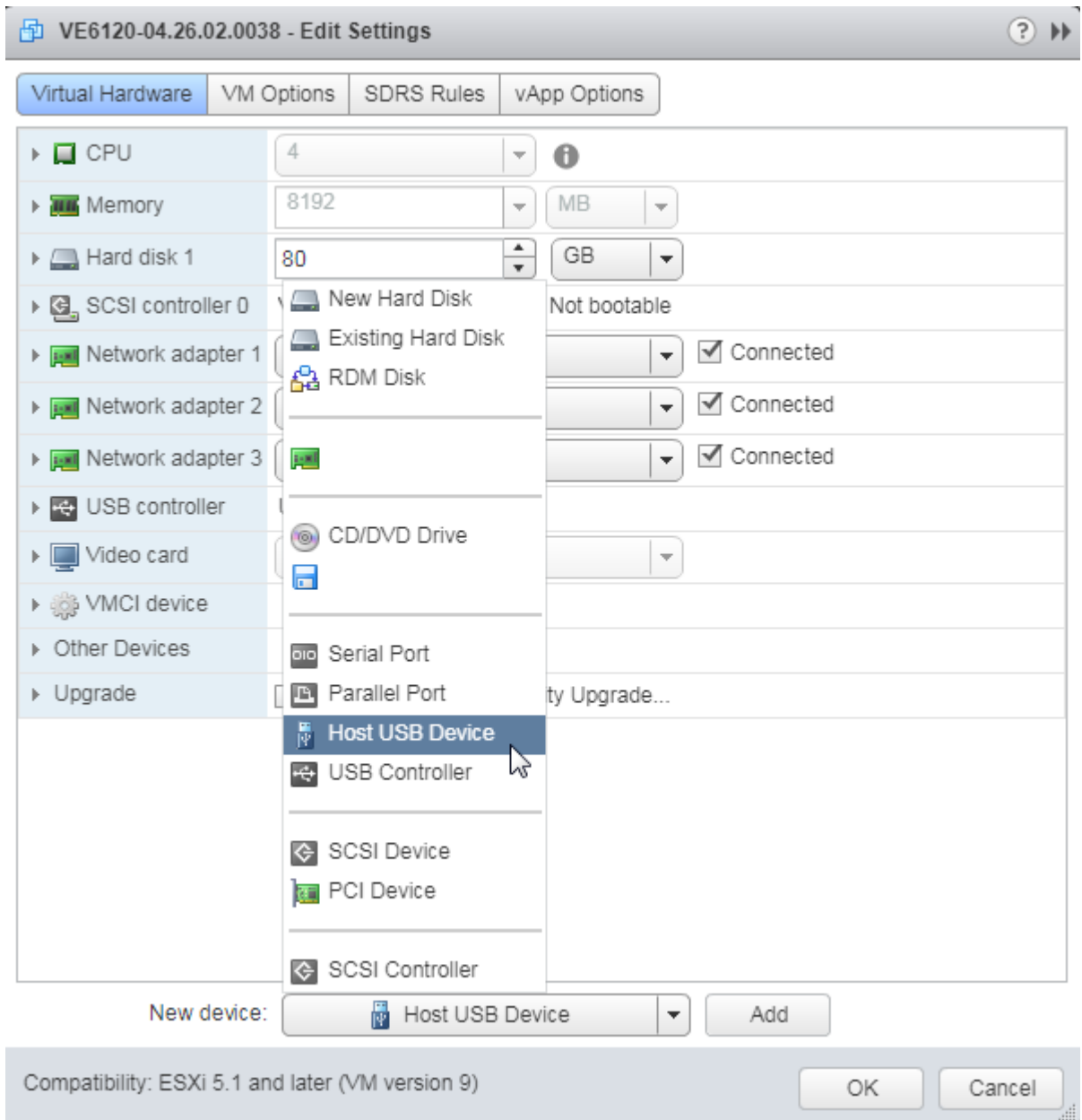

Figure 18: Host USB Device Selection

6   If running vSphere and a USB device has been inserted and is not assigned to another guest, the **USB Device** option will be listed. Select that option and click **OK**.

The **USB Device** dialog appears. The dialog lists all USB devices plugged into the host that are not assigned to guest operating systems.

7   Select a USB Flash drive (as other devices are not supported by VE6120), and click **OK**.

The **Ready to Complete** dialog appears.

8   Review the settings and then click **Finish** to add the USB device to VE6120 or click **Cancel** to abort the operation.

The **Virtual Machine Properties** dialog displays that the USB device is in the process of being added to the virtual machine. The new USB device will be shown in bold and "adding" appears after the USB device name.

9   Click **OK** to save the configuration.

10 Open the VE6120 **Virtual Machine Properties** dialog from the main vSphere client screen and click the **Hardware** tab.

The USB device will be listed under **Hardware**. You can now use the USB flash drive on the VE6120 just as you would on a physical controller.

Managing Flash Memory

Follow these steps to manage flash memory:

1   Log into the ExtremeCloud Appliance using your credentials.

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

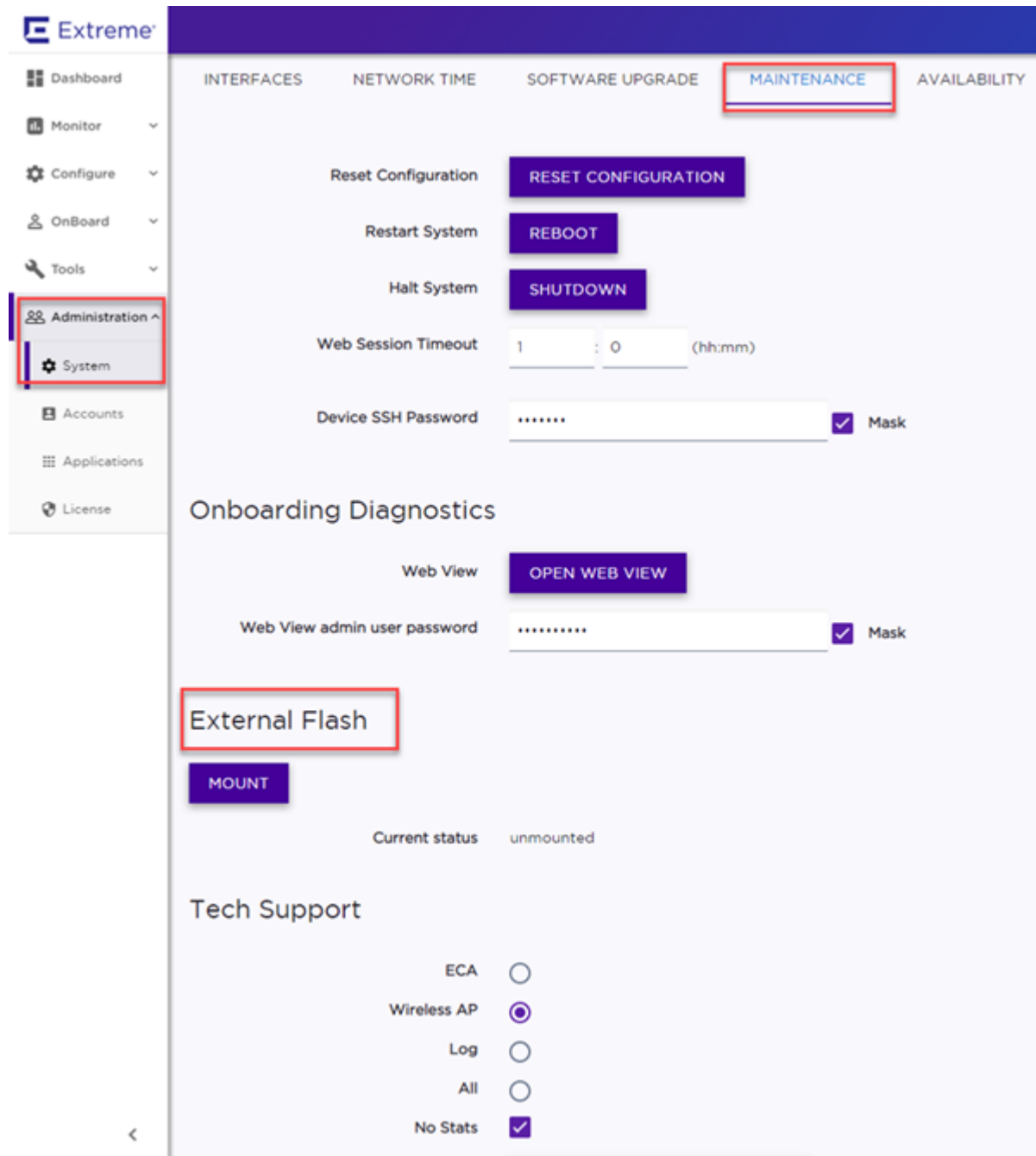Use the **Mount/Unmount** options to mount and unmount flash memory respectively.

Figure 19: Flash memory maintenance window

Removing the Flash Drive

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 using the vSphere client. Within a few seconds of the USB flash drive being assigned to it, the VE6120 will detect the flash drive and mount it for use.

1 When you are ready to remove the USB Flash drive, click **Un-Mount** from the Maintenance page.
2 Remove the drive.
3 You can delete the USB flash drive from the VE6120's **Virtual Machine Properties** dialog after unmounting it from the VE6120 appliance.

Activating the ExtremeCloud Appliance

Activating the Virtual Appliance requires an activation key that must be obtained from Extreme Networks Support. The activation key can be permanent or temporary depending on the license you have obtained.

To activate the Virtual Appliance:

1 Log in to the ExtremeCloud Appliance.
2 In the left pane, from the **Administration** drop-down, select **License**.

   The License page with the License Summary is displayed.
3 Enter the activation key in the Activation Key field and click **Apply**.

   There is also a field for Capacity Key if you have a permanent license for the ExtremeCloud Appliance. The capacity key is used for enhancing the capacity of the appliance to manage devices.

   To obtain the capacity key:

   1 Contact Extreme Networks Support.
   2 Enter the capacity key in the Capacity Key field and click **Apply**.

   The permanent license key and the capacity key is applied and the ExtremeCloud Appliance is activated.

For more information on licensing, refer to the ExtremeCloud™ Appliance's User Guide.

4 Configuring vSwitches for the Virtual Appliance

Creating a New Virtual Switch or Port Group on the ESXi Server
Configuring the Virtual Switch for Promiscuous Connections

The Virtual Appliance has some specific requirements on the virtual switches (vSwitch) to which its data plane ports are connected. This section explains how to create a vSwitch on an ESXi host that satisfies these requirements.

This does not replace the vSphere ESXi documentation. The procedures described in this section assume that you have already logged into the vSphere client using credentials that grant full administrative access to the vSphere ESXi host server.

Creating a New Virtual Switch or Port Group on the ESXi Server

This is an optional procedure since it is possible to reconfigure the virtual switch created by default when ESXi is installed to support VLANs or another acceptable custom vSwitch might be configured on the host. However, using separate vSwitches for the data plane traffic helps to isolate that traffic from other virtual devices and permits the switch to be configured specifically to meet the needs of the VE6120.

> **Note**
> Alternatively, it is also possible to define more than one network (Port Group) on a single vSwitch. All networks on the same vSwitch share the NICs assigned to the vSwitch.

To create the new switch or port group:

1   Login to the vSphere web client. For more information, see Accessing the Virtual Appliance Console on page 17.
2   On the vSphere web client screen, in the left pane, click on the vSphere server's IP address or host name. The **Configure** tab displays on the right pane.
3   On the right pane, select **Networking** > **Virtual switches**.

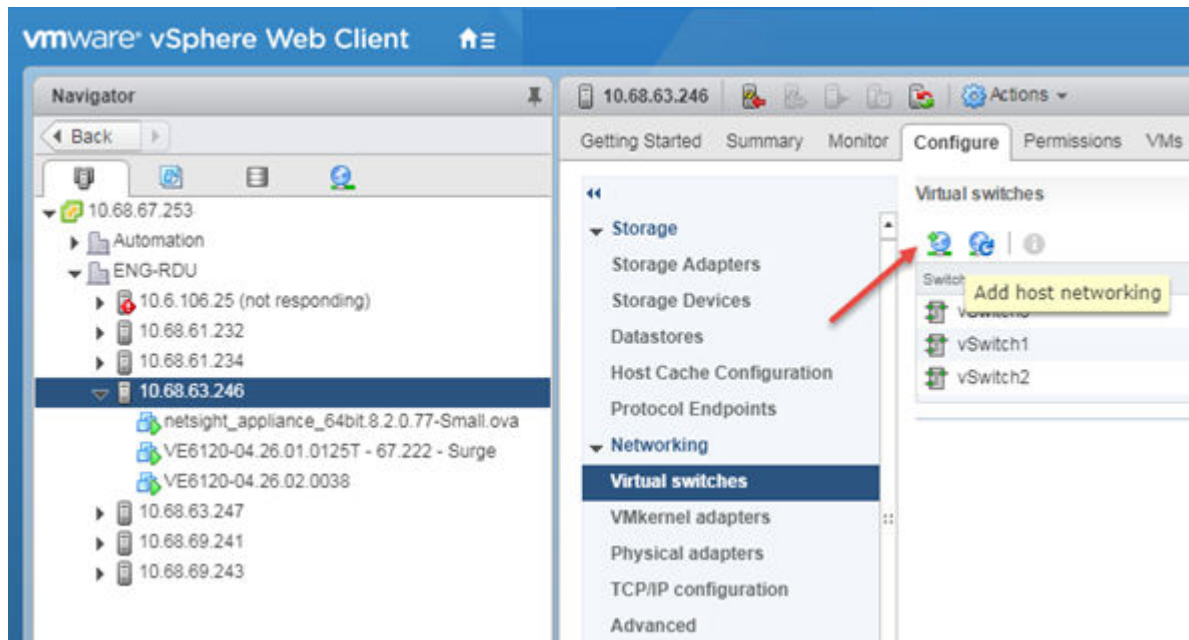4   Select the globe icon **Add host networking**.

Figure 20: Adding a virtual switch

5   Select the connection type: Select **Virtual Machine Port Group for a Standard Switch**.

6 **Select target device:**. You can create a new switch or create a new port group on an existing switch.

- To create a port group on an existing switch:

    1 Select **Select an existing standard switch**.

    2 Click **Browse**, and select an switch from the list.

    3 Click **Next**.

- To create a new switch:

    1 Select **New standard switch**.

    2 Click **Next**.

    3 Select Assigned adapters or click plus sign to add new adapters.

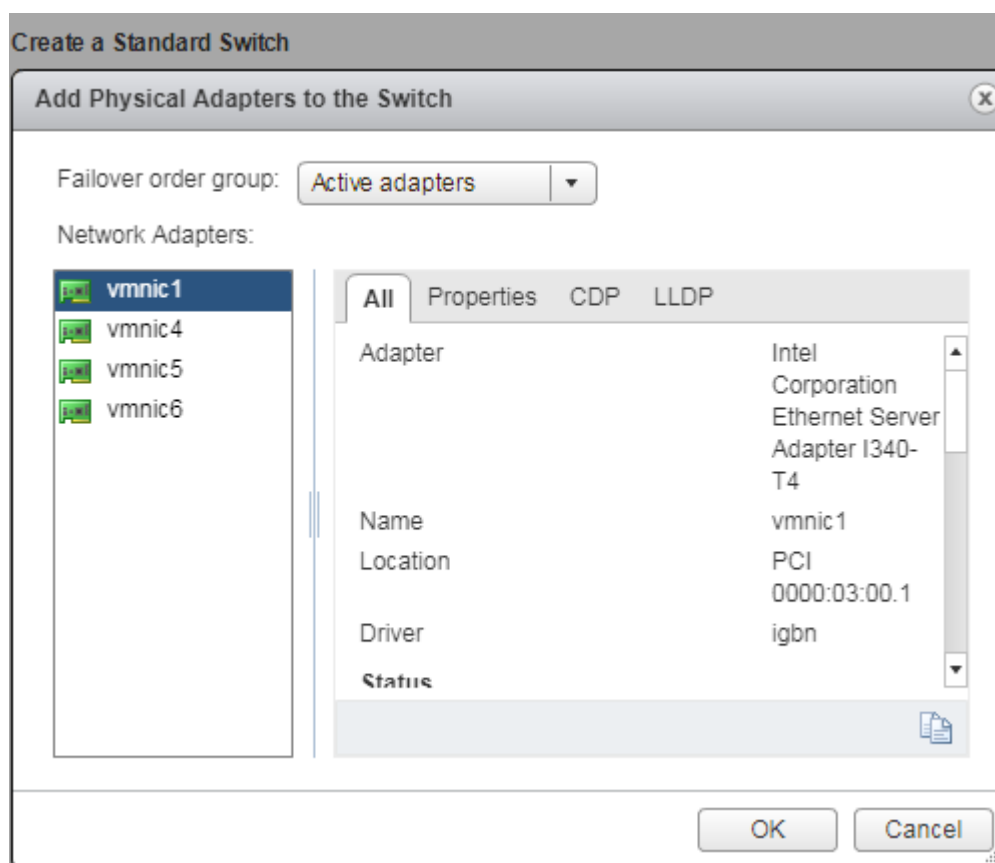   4 Select the appropriate adapter, and click **OK**.

Figure 21: Adding network adapters

    5 On the **Create a Standard Switch** dialog, click **Next**.

7 **Connection settings:**

- Provide a Network label for the switch or port group.

- VLAN ID — **All (4095)**

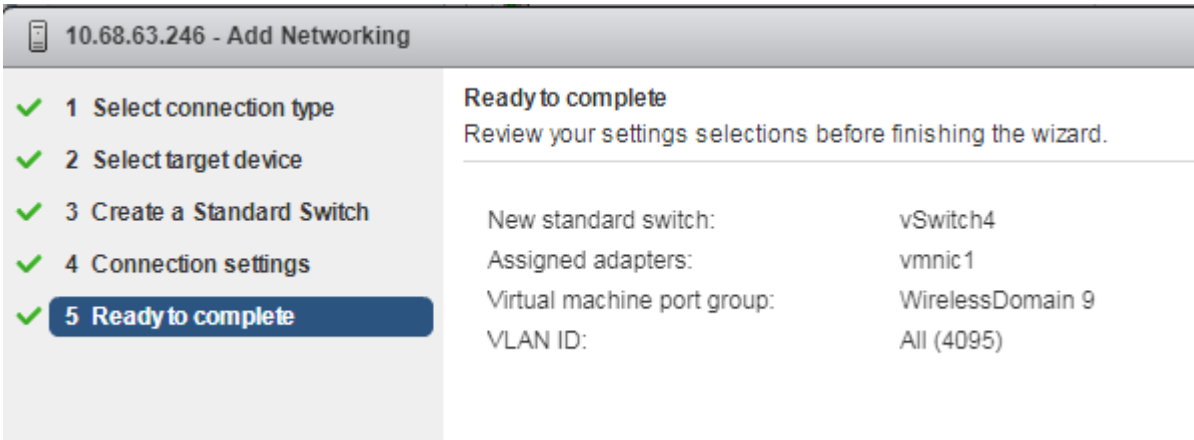8 **Ready to complete:** Review the settings and click **Finish**.

Figure 22: Ready to complete

9 The new switch is listed in the **Virtual switches** list. A diagram of the Port Groups and Physical Adapters displays.
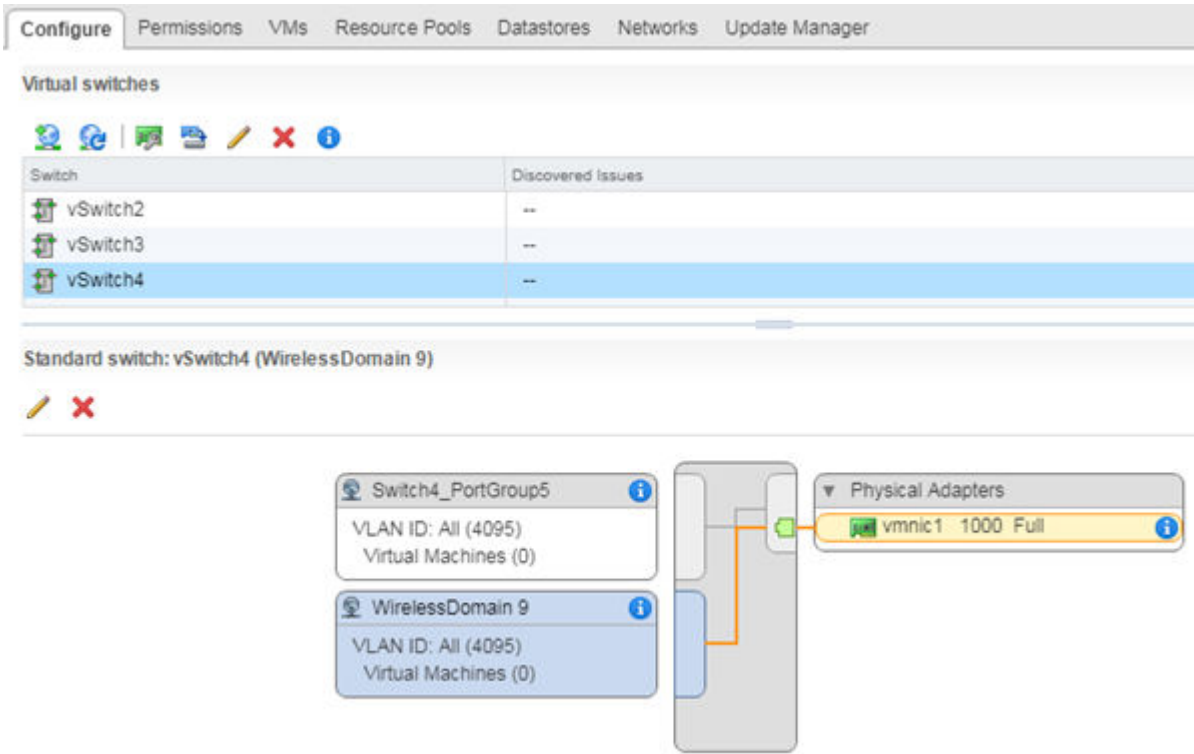

Figure 23: Switch Diagram

Next, configure the virtual switch for promiscuous connections.

Configuring the Virtual Switch for Promiscuous Connections

ESXi virtual switches collect ports into port groups. Every virtual switch must have at least one port group and one is created automatically by ESXi when the vSwitch is created. The VE6120's data plane ports always operate in promiscuous mode so changing this default is mandatory. The new virtual

switch and port group will be configured to accept MAC address changes and forged transmits, but this may not be necessary.

To change the security settings of a virtual switch:

1   Login to the vSphere web client host network. For more information, see Accessing the Virtual Appliance Console on page 17.
2   On the vSphere web client screen, in the left pane, click on the vSphere server's IP address or host name. The **Configure** tab displays on the right pane.
3   On the right pane, select **Networking** > **Virtual switches** and select a switch from the list.
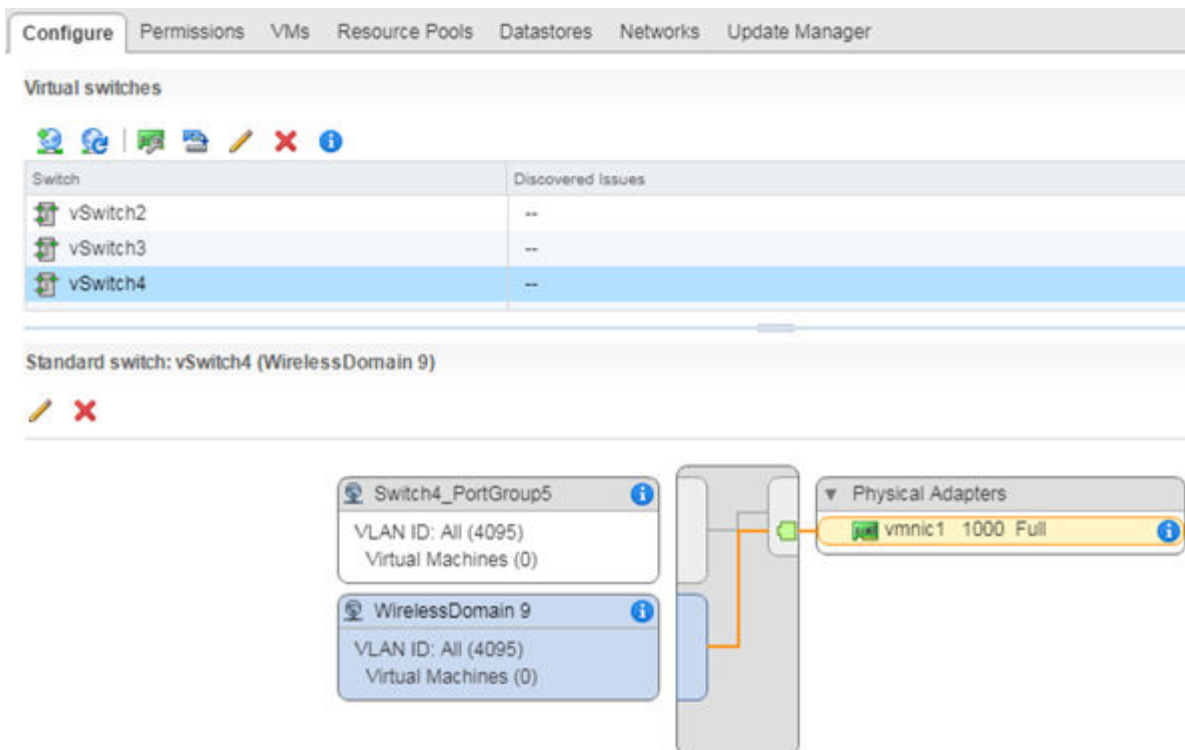

Figure 24: Switch Diagram

4   Select a pencil icon to edit properties:

- To configure properties for the entire switch, select switch in the switch list, then select the pencil icon above the list.
- To configure properties for a port group, select the port group in the diagram, then select the pencil icon above the diagram.
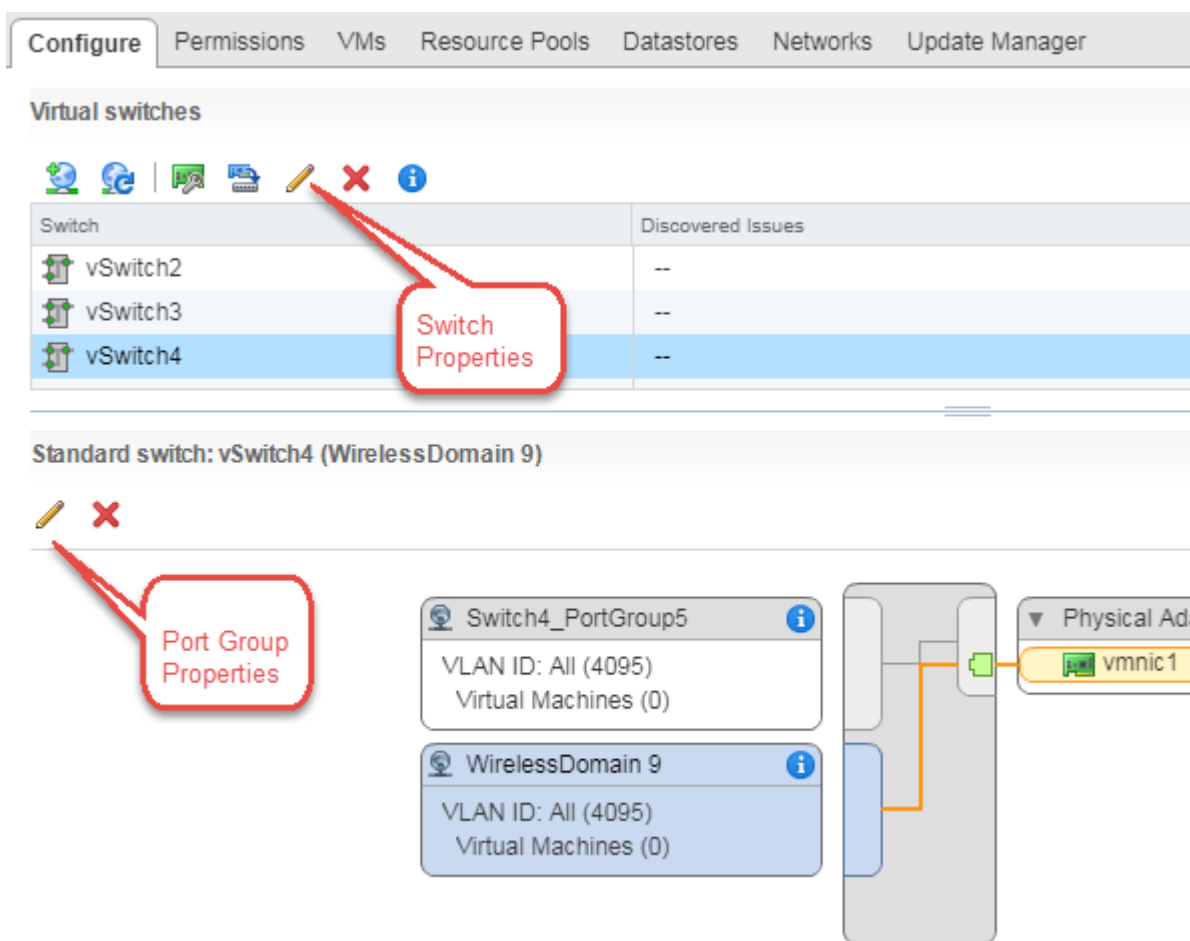

Figure 25: Editing properties

5   On the **Edit Settings** dialog, select the **Security** tab, and set all options to **Accept**.
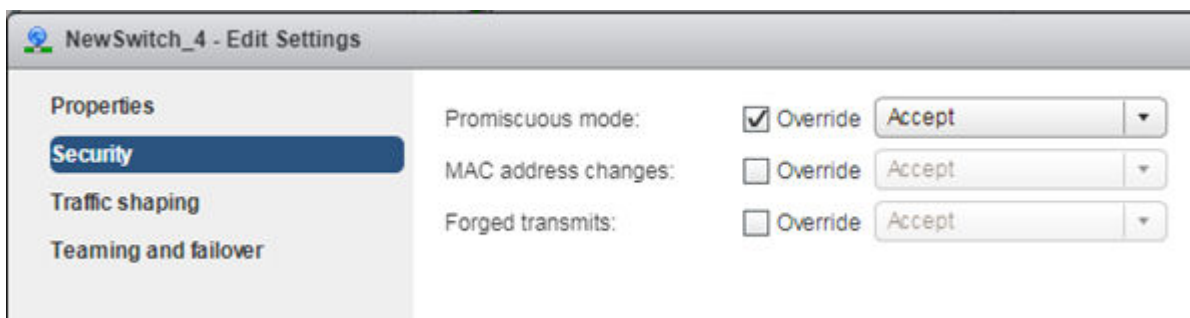
6   Click **OK** to close the **Edit Settings** dialog.

Figure 26: Promiscuous mode setting

5 Configuring a Virtual Machine to gain more Networking Performance

Configuring a virtual machine to gain more networking performance allows you to increase the networking throughput, especially if you use 10Gbps or faster NICs on the server.

> **Note**
> Perform this task after every .ova deployment since the settings cannot be exported with an .ova image.

vSphere uses single receive thread and single transmit thread, regardless of the number of virtual devices configured on it. It is necessary to scale vSphere to prevent packet loss, core overload, and degraded performance.

This configuration creates a special transmit queue on the host server (ESXi) per appliance data plane networking interface. If you do not use both Port 1 and Port 2 on the appliance, the configuration can be applied on only the port that is being used.

If any particular vNIC is overloaded, you can configure additional cores to parallelize the threads by using the `ethernetX.ctxPerDev` command in the virtual machine file.

> **Note**
> Use this command only on vNICs that will handle high packet loads.

To configure and enable the `ethernetX.ctxPerDev` command on a vNIC:
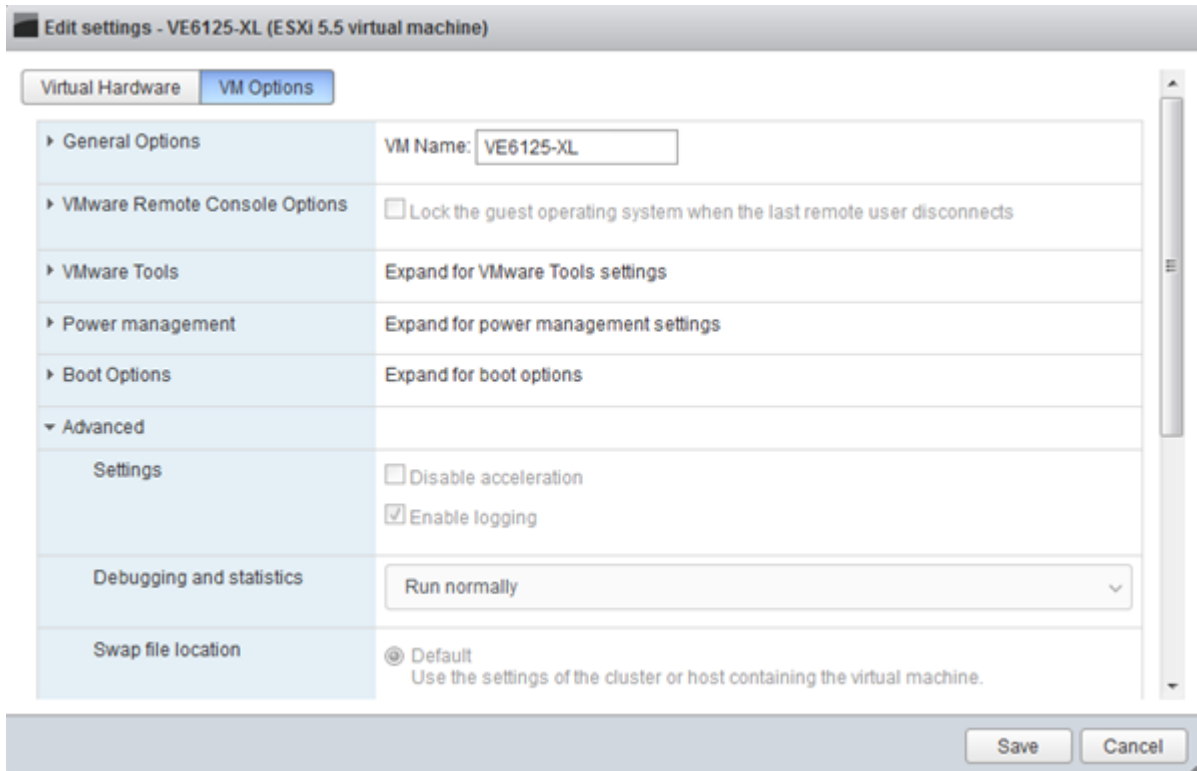
1   Shutdown the virtual machine.

2   Select **VM Options**.

Figure 27: VM Options tab

3   Expand the **Advanced** drop-down.

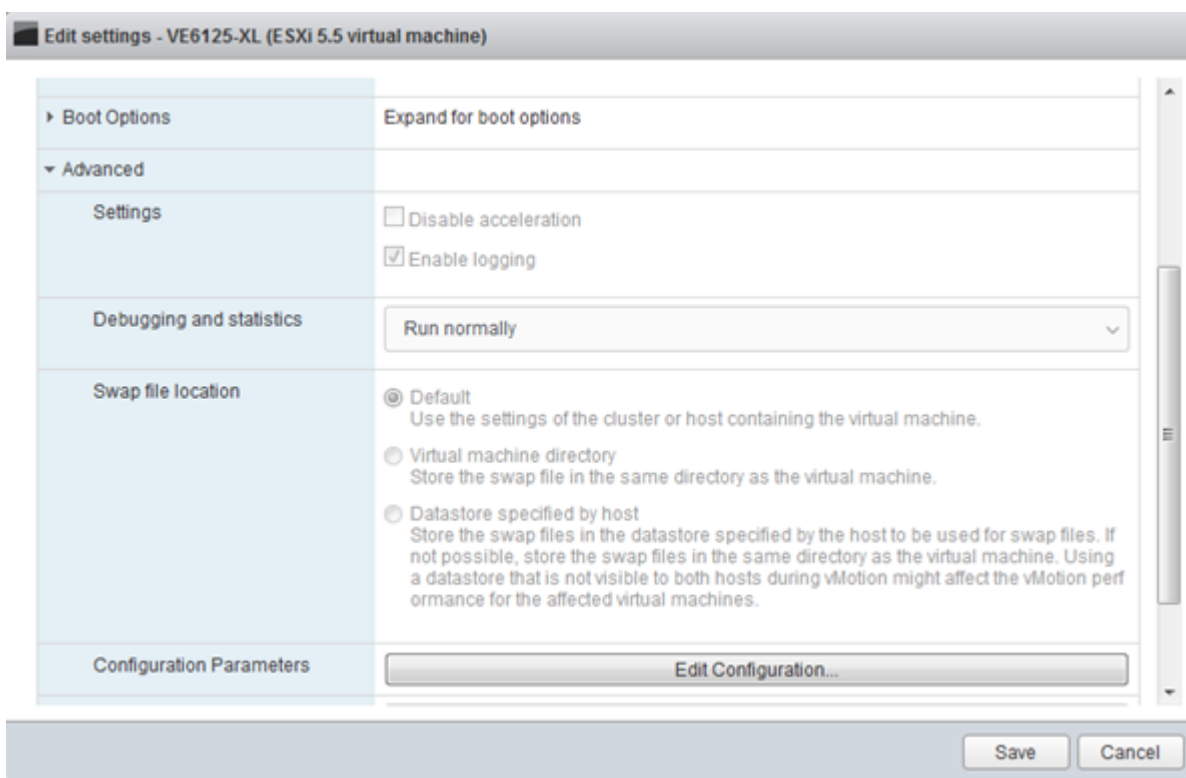4   Click **Edit Configurations** next to the **Configuration Parameters** option.

Figure 28: Edit Configuration option

The **Configuration Parameters** window opens.
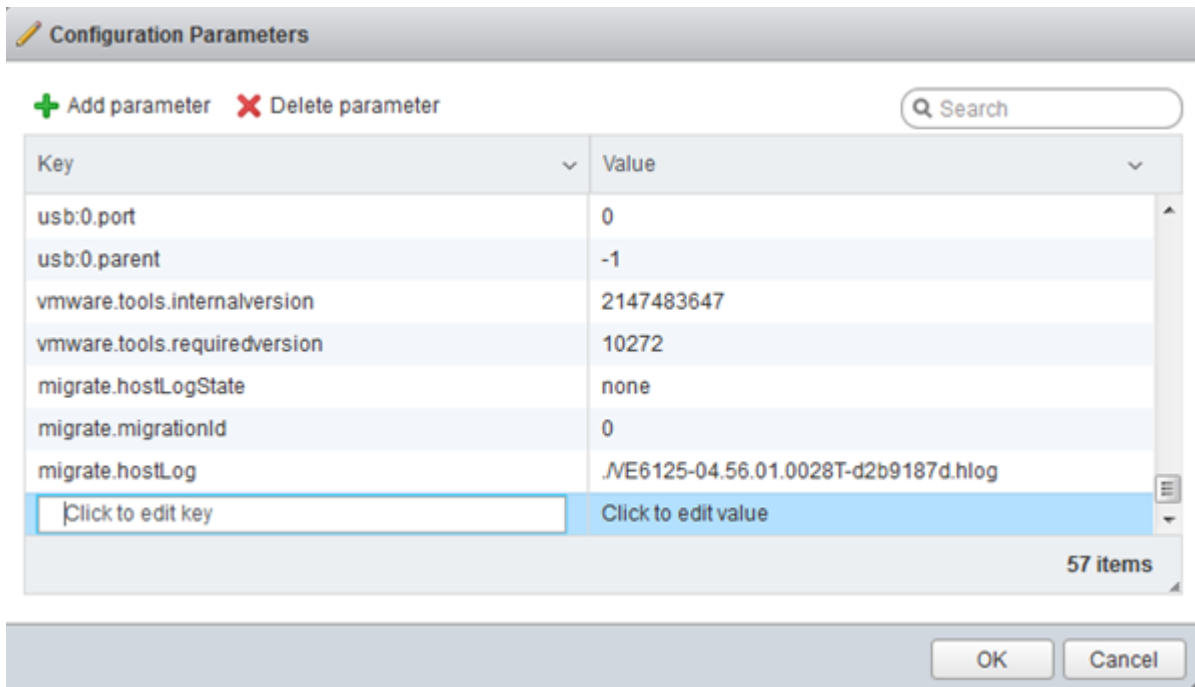
5   Click **Add parameter** to add an entry.

Figure 29: Configuration Parameters window

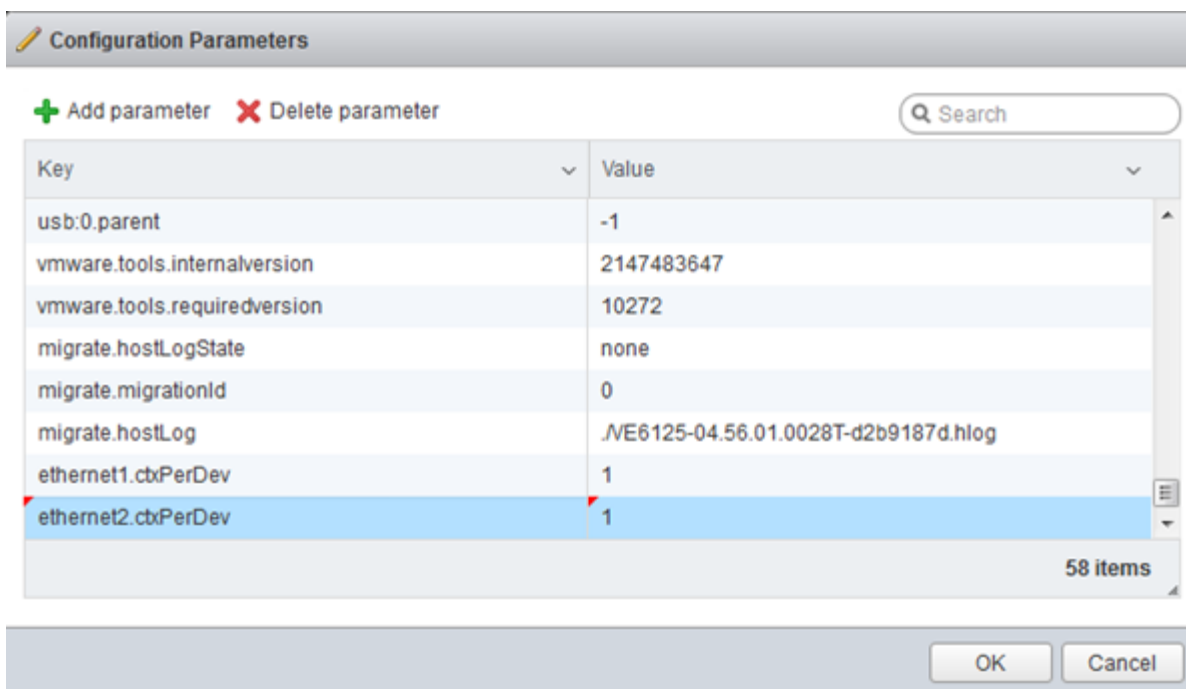6   Set the following parameters in the **Configuration Parameters** window.

Table 6: Configuration parameters entries

Key	Value
For Port 1: • ethernet1.ctxPerDev	1
For Port 2: • ethernet2.ctxPerDev	1

Note

The "X" in `ethernetX.ctxPerDev` command is replaced with the vNIC number.

7   Click **OK** to add the configuration parameter.

8   Click **Save** to save the configuration parameter.

9   Power on the virtual machine.

6 Shutting down and restarting a Virtual Machine

Shutting down and restarting a Virtual Machine using the Graphical User Interface (GUI)
Shutting down and restarting a Virtual Machine on a ESXi server

You need to shut down a virtual machine before configuring it to gain more networking performance. This 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 Accessing the Virtual Appliance Console on page 17.

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

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.

Shutting down and restarting a Virtual Machine using the Graphical User Interface (GUI)

You can also shut down and restart the virtual machine using the GUI.

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

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.

Shutting down and restarting a Virtual Machine on a ESXi server

You can shut down and restart a virtual machine through the ESXi server as well.

To shut down and restart a virtual machine through ESXi:

1   To shut down the virtual machine, right click the virtual machine you need to shut down, listed under **Virtual Machines**, select **Guest OS** > **Shut down**.

2   To restart the virtual machine, right click the virtual machine you need to restart, listed under **Virtual Machines**, select **Guest OS** > **Restart**.
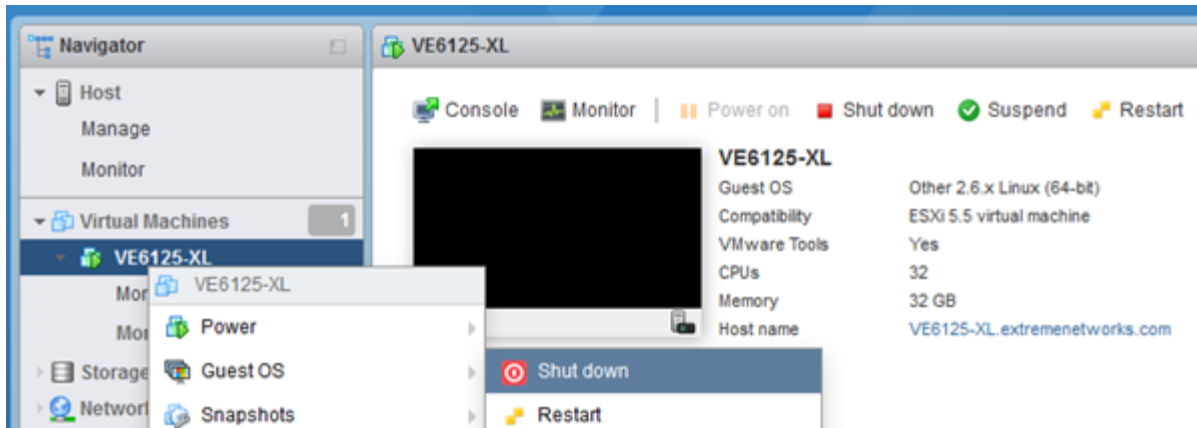

Figure 30: Shut down or restart a virtual appliance through ESXi server

3   You can also shut down or restart a virtual machine by directly selecting the **Shut down** or **Restart** option on the ESXi server.