WatchGuard XTMv Setup Guide

Fireware v11.10

All XTMv Editions

Copyright and Patent Information

Printed in the United States of America.

Revised: October 30, 2015

Updated for: Fireware v11.10.4

U.S. Patent Nos. 6,493,752; 6,597,661; D473,879. Other Patents Pending.

Complete copyright, trademark, patent, and licensing information can be found in the WatchGuard product documentation. You can find this document online at:
http://www.watchguard.com/help/documentation/

Notice to Users

Information in this guide is subject to change without notice. Updates to this guide are posted at:

http://www.watchguard.com/help/documentation/xtm.asp

ABOUT WATCHGUARD

WatchGuard offers affordable, all-in-one network and content security solutions that provide defense-in-depth and help meet regulatory compliance requirements. The WatchGuard XTM line combines firewall, VPN, GAV, IPS, spam blocking and URL filtering to protect your network from spam, viruses, malware, and intrusions. The new XCS line offers email and web content security combined with data loss prevention. WatchGuard extensible solutions scale to offer right-sized security ranging from small businesses to enterprises with 10,000+ employees. WatchGuard builds simple, reliable, and robust security appliances featuring fast implementation and comprehensive management and reporting tools. Enterprises throughout the world rely on our signature red boxes to maximize security without sacrificing efficiency and productivity.

For more information, please call 206.613.6600 or visit www.watchguard.com.

ADDRESS

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

SUPPORT

www.watchguard.com/support
U.S. and Canada +877.232.3531
All Other Countries +1.206.521.3575

SALES

U.S. and Canada +1.800.734.9905
All Other Countries +1.206.613.0895

XTMv Introduction

WatchGuard® Firebox and XTM security devices deliver unparalleled unified threat management, superior performance, ease of use, and value for your growing network. Our security subscriptions give you fully integrated protection from spyware, spam, viruses, worms, trojans, web-based exploits, and blended threats. From firewall and VPN protection to secure remote access, WatchGuard devices support a broad range of network environments.

This guide describes how to set up a WatchGuard XTMv security device as a virtual machine on aVMware ESXi host or Microsoft Hyper-V hypervisor environment.

Fireware

WatchGuard XTMv uses Fireware® OS. Each XTMv virtual machine includes Fireware OS and delivers exceptional protection against today's sophisticated threats, to make sure that your business stays connected. For more information about the features of Fireware OS, see the *Fireware Help*.

WatchGuard XTMv

A WatchGuard XTMv virtual machine can run on a VMware ESXi 4.1, 5.0, 5.1, 5.5, or 6.0 host, or on a Windows Server 2008 R2, Windows Server 2012, Hyper-V Server 2008 R2, or Hyper-V Server 2012.

You can use WatchGuard System Manager, Fireware Web UI, and the Command Line Interface (CLI) to manage an XTMv virtual machine, just as you manage any other Firebox or XTM device.

XTMv Limitations

XTMv supports most features available in Fireware OS, with the exception of a few features that are hardware-dependent.

Fireware features not supported on XTMv include:

- Active/active FireCluster in VMware ESXi environment (FireCluster is not supported for Hyper-V)
- Bridge mode network configuration
- Hardware diagnostics CLI commands
- Automatically save a support snapshot to a USB drive
- Automatically restore a saved backup image from a USB drive

To work correctly, some Fireware networking features require that you configure the virtual switch on your network in promiscuous mode. Because Hyper-V virtual switches do not support promiscuous mode, these features are not supported for XTMv in a Hyper-V environment:

- Drop-in mode network configuration
- Network bridge
- Mobile VPN with SSL, with the **Bridged VPN Traffic** setting

XTMv supports the features that require promiscuous mode only when deployed on a VMware ESXi server, with promiscuous mode enabled on the connected virtual network adapters.

To use multiple VLANs on a single interface on an XTMv device in an ESXi environment, configure the vSwitch for the XTMv VLAN interface to use VLAN ID 4095 (All).

To configure an active/passive FireCluster in an ESXi environment, you must enable promiscuous mode on the vSwitch interface that connects to the FireCluster management interface. We recommend that you enable promiscuous mode on any vSwitch that connects to any FireCluster interface to enable the cluster to support all networking features.

XTMv Licensing

XTMv devices are licensed in several different editions, which provide different levels of scalability and performance:

- Small Office Edition
- Medium Office Edition
- Large Office Edition
- Datacenter Edition

When you activate your XTMv device, a feature key is generated. The feature key enables the Fireware capabilities for the XTMv edition you have licensed. The feature key is installed on the XTMv virtual machine during setup. You can also use a feature key to upgrade from one XTMv edition to another.

For a comparison of the features and capabilities of each XTMv edition, see the **Products** section of the WatchGuard web site at www.watchguard.com.

XTMv Installation Overview

The installation prerequisites and steps to deploy an XTMv virtual machine depend on which hypervisor environment you use.

Before you begin, download the XTMv .ovf template file or .vhd virtual hard disk file, and the WatchGuard System Manager software from the *Articles and Software* section of the WatchGuard Portal.

VMware ESXi

For XTMv on ESXi, WatchGuard distributes XTMv as a WatchGuard XTMv virtual appliance Open Virtual Machine Format (.ovf) file.

To deploy an XTMv virtual appliance on an ESXi host:

1. Use the VMware vSphere Client to deploy the XTMv virtual appliance to an ESXi host.
2. Power on the XTMv virtual machine.
3. Connect to the XTMv virtual machine and use the Web Setup Wizard to set up a basic configuration.
4. Allocate additional resources to the XTMv virtual machine.

For complete instructions, see "XTMv Setup on VMware ESXi" on page 5.

You can also configure two ESXi virtual machines as a FireCluster on ESXi.

Microsoft Hyper-V

For XTMv on Hyper-V, WatchGuard distributes XTMv as a WatchGuard XTMv virtual hard disk (.vhd) file.

To deploy an XTMv virtual hard disk in a Hyper-V environment:

1. Use Hyper-V Manager or System Center VMM to deploy the XTMv virtual machine and select the .vhd file to use.
2. Assign network adapters, and power on the XTMv virtual machine.
3. Connect to the XTMv virtual machine and run the Web Setup Wizard to set up a basic configuration.
4. Allocate additional resources to the XTMv virtual machine.

For complete instructions, see "XTMv Setup on Microsoft Hyper-V" on page 23.

WatchGuard Setup Wizards

This guide describes how to use the Fireware Web Setup Wizard to create the initial configuration on a deployed XTMv virtual machine. To run the Web Setup Wizard, you can connect to the XTMv virtual machine from a computer on either the external or trusted network.

If you have installed WatchGuard System Manager on a computer on the XTMv device trusted network, you can use the Quick Setup Wizard in WatchGuard System Manager instead of the Web Setup Wizard to discover the XTMv virtual machine and set up the basic device configuration.

XTMv Setup on VMware ESXi

This section describes how to deploy and configure a WatchGuard XTMv virtual machine on a VMware vSphere ESXi host.

Installation Prerequisites

The environment where you install the XTMv virtual device must meet these requirements:

- **VMware**
  - You must have a VMware vSphere Hypervisor/ESXi 4.1 Update 2 (or later) or ESXi 5.0, 5.1, 5.5, or 6.0 host installed on a server that supports your ESXi version.
  - Your VMware vSphere/ESXi software must be updated to the latest patch level.
  - You must install the VMware vSphere Client on a supported Windows computer.
    In the procedures in this document, we use the vSphere Client to deploy, configure, and provision the XTMv virtual machine on an ESXi 5.1 host. You can use vCenter Server instead of the vSphere Client.

Note

Some WatchGuard customers have successfully used vMotion to migrate an XTMv virtual machine between ESXi hosts while the XTMv virtual machine is powered on and passing traffic. However we recommend that you power down the XTMv virtual machine, if possible, before you migrate it between ESXi hosts.

- **Hardware**
  - The hardware requirements for XTMv are the same as the hardware requirements for VMware ESXi.
    For information about VMware hardware compatibility, see the VMware Compatibility Guide at http://www.vmware.com/resources/compatibility/search.php.
  - Each XTMv virtual machine requires 3 GB of disk space.

XTMv Installation

Before You Begin

To prepare for your installation, make sure you have these things:

- VMware ESXi 4.1 Update 2, 5.0, 5.1, 5.5, or 6.0 host installed on a supported server platform
- VMware vSphere Client installed on a Windows computer
- XTMv device serial number
  You receive the serial number when you purchase the XTMv virtual device.
- WatchGuard XTMv virtual appliance Open Virtual Machine Format (OVF) file
  The file name is xtmv_<version>.ova, where <version> is the Fireware version.
- *(optional)* WatchGuard System Manager v11.7.3 or higher (WatchGuard System Manager v11.8.1 or higher is required to configure FireCluster)

Download the `XTMv.ovf` template file and the WatchGuard System Manager software from the *Software Downloads* page on the WatchGuard website.

Installation Overview

To complete the initial installation of your XTMv virtual machine, perform these procedures as described in the subsequent sections:

1. In the VMware vSphere Client, deploy the XTMv virtual appliance to the ESXi host and power on the XTMv virtual machine.
2. Connect to the XTMv virtual machine and run the Web Setup Wizard to set up a basic configuration.
3. Allocate additional resources to the XTMv virtual machine.

This guide describes how to use the Web Setup Wizard to create an initial configuration for your XTMv device. If you have installed WatchGuard System Manager on a computer on the XTMv device trusted network, you can use the Quick Setup Wizard in WatchGuard System Manager instead of the Web Setup Wizard to discover the XTMv virtual machine and set up the basic device configuration.

Note

To activate your XTMv device from the Web Setup Wizard, you must have the device serial number. You cannot use a serial number that ends with 000000000, which is the serial number for an unactivated device.

Network Considerations

When you deploy the XTMv virtual appliance, it is initially configured with two active interfaces.

External interface
The external interface, Interface 0, is set up by default to request an IP address from a DHCP server. If you want to connect to this interface for the initial device configuration, you must map this interface to a destination network that has a DHCP server.

Trusted interface
The trusted interface, Interface 1, has a default IP address of 10.0.1.1.

When you deploy the XTMv virtual appliance to the ESXi device, you map each of these interfaces to a destination network.

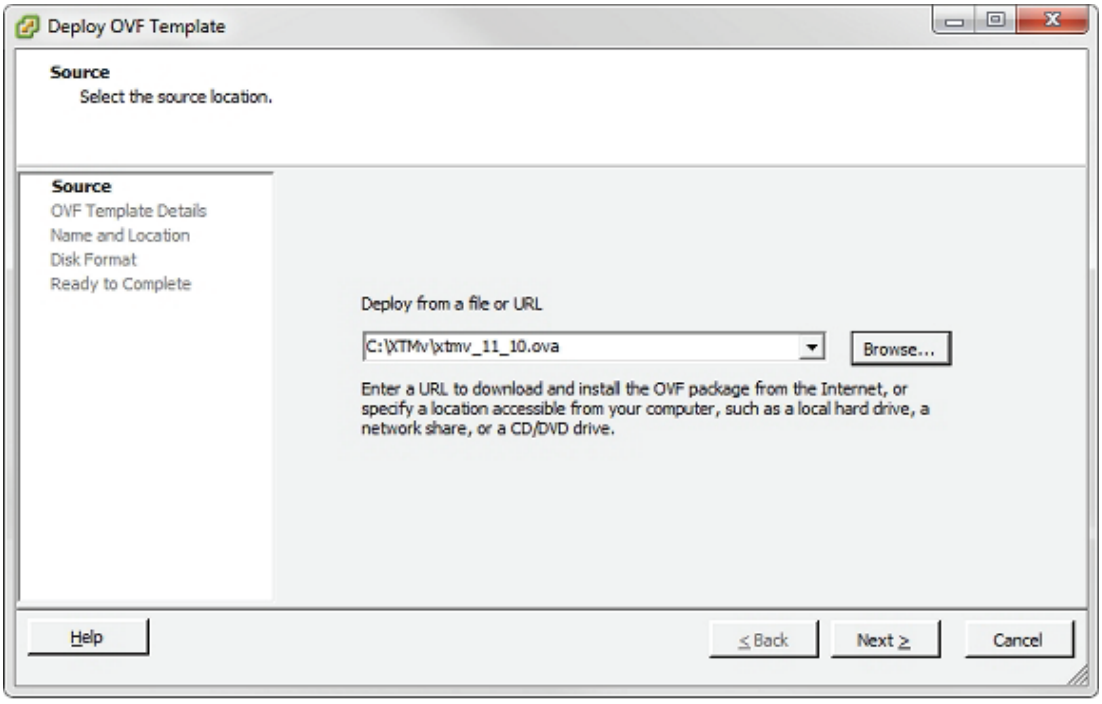
After you deploy the XTMv virtual machine, you can enable and configure additional XTMv device network interfaces. For additional interfaces to operate, you must configure the XTMv virtual machine in the vSphere Client or vCenter Server, and add the number of network adapters you want to enable in the XTMv device configuration.

Deploy the XTMv Virtual Appliance

You can use the vSphere Client, vSphere Web Client, or vCenter Server to deploy the XTMv virtual appliance (OVF template file). These procedures show how to use the vSphere client.

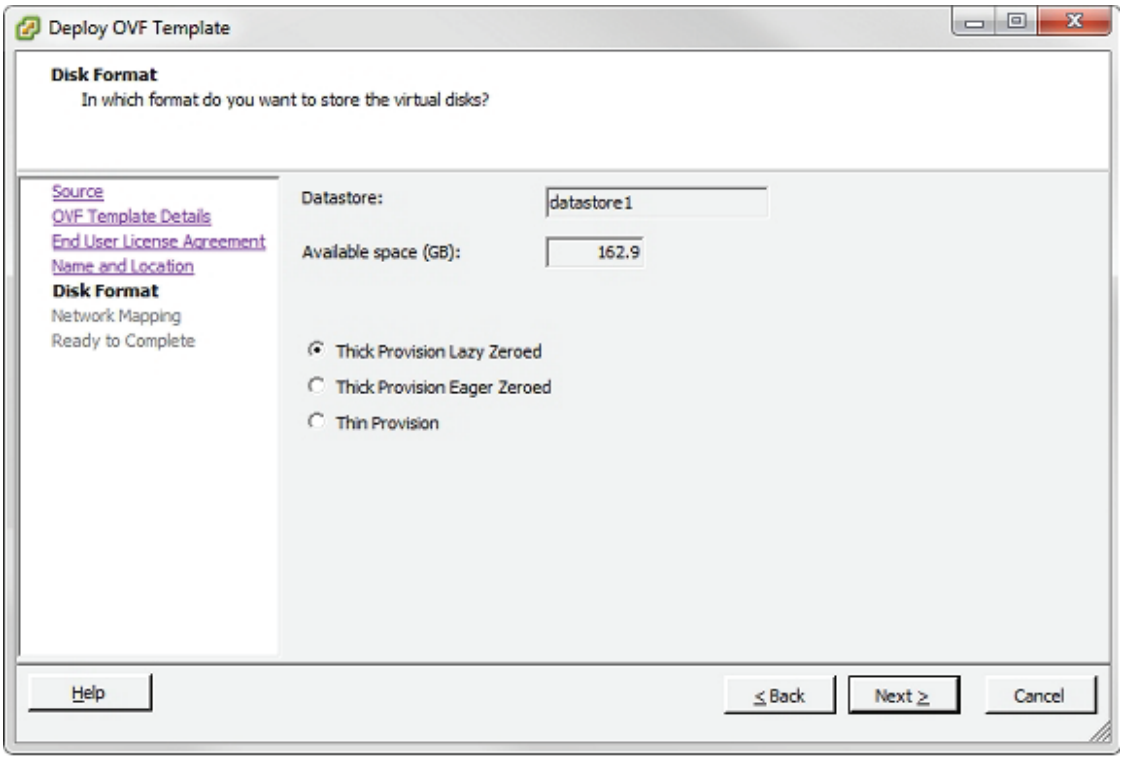
To use the vSphere Client connected to an ESXi host:

1. Launch the vSphere Client and log in to the ESXi host with administrator credentials.
2. In the vSphere client, select **File > Deploy OVF Template**.



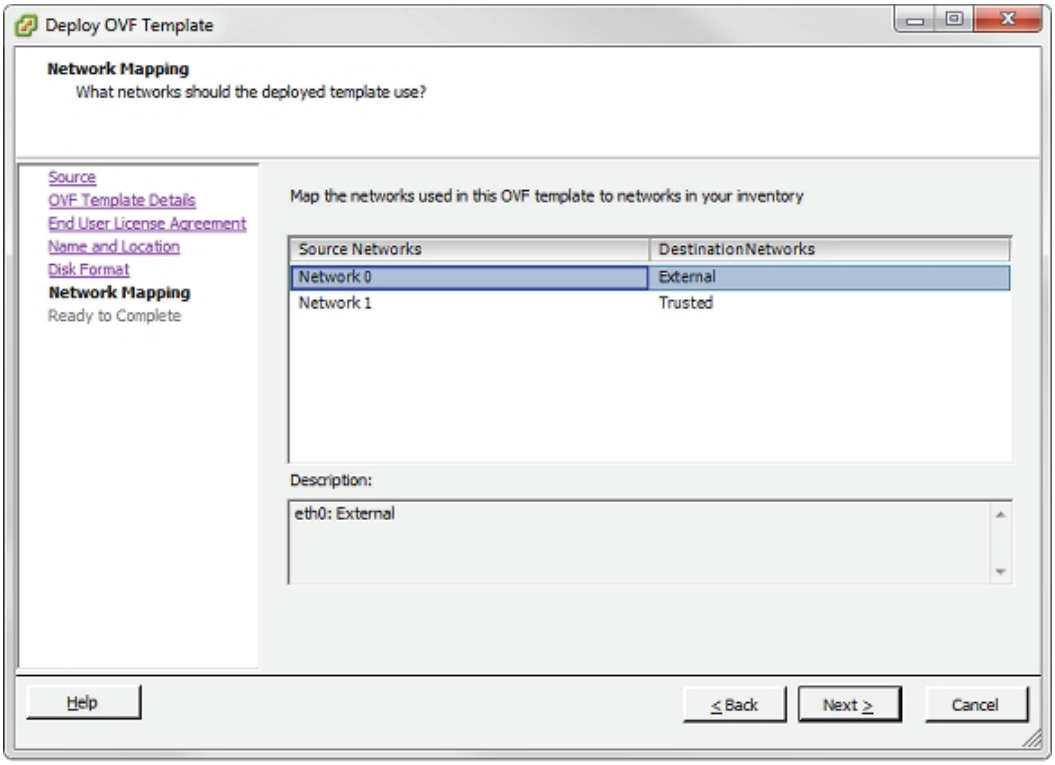
3. **Browse** to the location where you saved the WatchGuard XTMv OVF template file, xtmv_<*version*>.ova. Click **Next**.
The XTMv OVF Template Details page appears.

4. Click **Next**.
   The End User License Agreement appears.
5. Review the End-User License Agreement. Click **Accept**. Click **Next**.
   The Name and Location page appears.
6. In the **Name** text box, type a name for this virtual device. Click **Next**.
7. If your ESXi host has more than one resource pool, select the resource pool for this template.
   If you selected a resource pool in the vSphere Client inventory tree before you started to deploy the OVF template, you do not see this step.
8. Click **Next**.
   The Disk Format page appears.



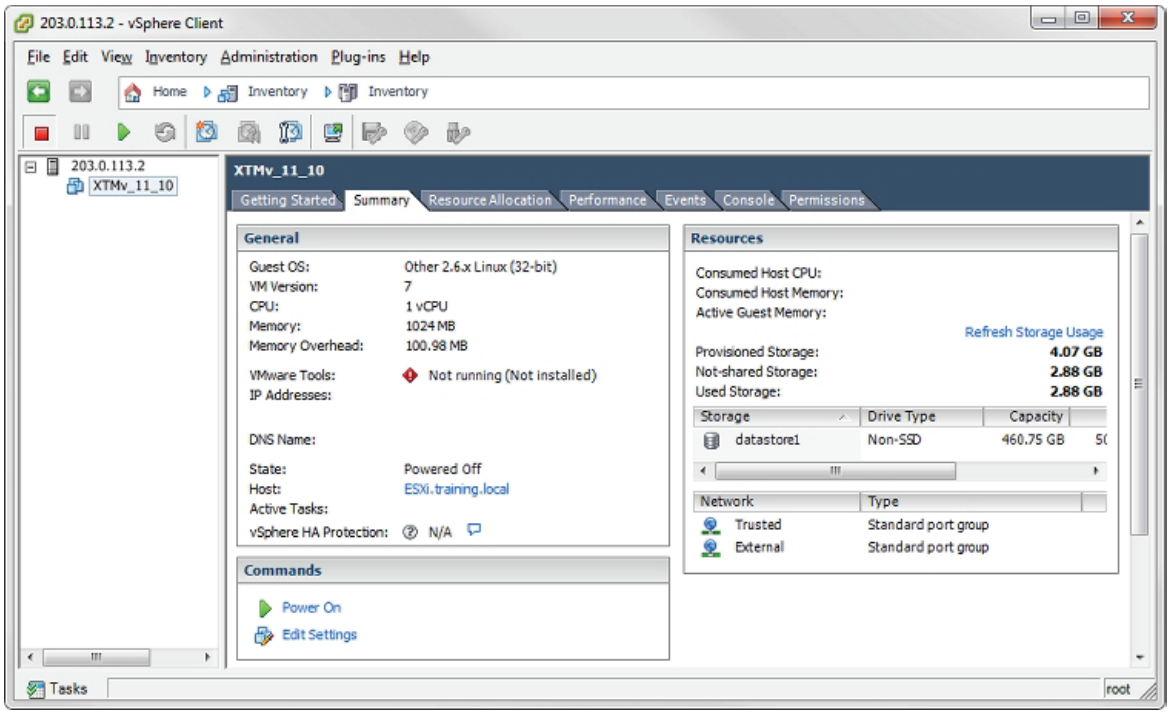
9. Select the storage format for the virtual disks.
   We recommend that you select one of the **Thick provision** formats to allocate all storage immediately.

10. Click **Next**.
    The Network Mapping page appears.



11. In the **Destination Networks** column, select the networks to map to Network 0 (eth0: External) and Network 1 (eth1: Trusted).
12. Click **Next**.
    The Ready to Complete page appears.
13. Review the settings. Click **Back** to change any settings, if necessary.
14. Click **Finish** to deploy the template.
    The virtual machine is created. This can take a few minutes.

The deployed XTMv virtual machine appears in the vSphere Inventory.



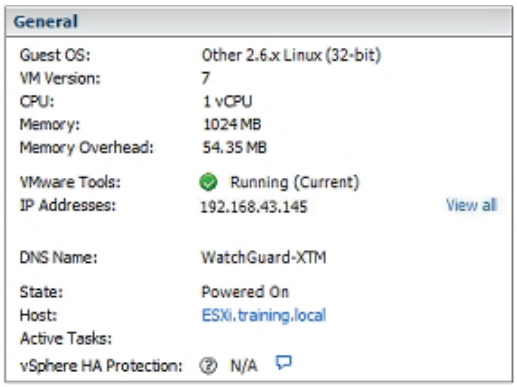
If there are additional resources that you want to allocate to this virtual machine, you can allocate those resources now, before you power on the virtual machine. Or, you can add resources later. You do not have to allocate additional resources to create a basic Fireware configuration. For more information about how to allocate additional resources, see “ESXi Resource Allocation” on page 15.

Power On the XTMv Virtual Machine

Next, you power on the XTMv virtual machine. When you initially power it on, the XTMv virtual machine automatically sends a DHCP broadcast to request an IP address for the external interface. If a DHCP server is configured on the external network, the XTMv external interface receives an IP address.

To power on the XTMv virtual machine:

1. In the **vSphere Client Inventory** tree, select the virtual device.
2. Select the **Summary** tab.
3. In the **Commands** section, select **Power on**.
   The XTMv virtual machine is powered on with factory default settings.
4. After the virtual machine is powered on, and if a DHCP server exists on the XTMv external network, the **IP Addresses** setting shows the IP address assigned to Interface 0. If an address is not assigned to the XTMv external network, the **IP Addresses** setting shows the default IP address for Interface 1, 10.0.1.1.



5. Click **View all** to see all assigned IP addresses.

XTMv Device Factory Default Settings

When you power on the XTMv virtual machine for the first time, the XTMv device starts with these factory default settings:

- The XTMv device has two active interfaces: external and trusted.
- The trusted interface has the IP address 10.0.1.1.
- The external interface is configured to receive an IP address through DHCP.
- The trusted interface is not configured to assign IP addresses with DHCP.
  This is different than the default setting for other Firebox and XTM devices.
- Both the trusted and external interfaces accept management connections.
  This is different than the default setting for other Firebox and XTM devices.
- The **admin** account passphrase is `readwrite`.
- The serial number for an unactivated XTMv device ends with 000000000.
  You assign the actual serial number during device activation.

Use the Web Setup Wizard to Create a Basic Configuration

The Fireware Web Setup Wizard is almost the same for an XTMv virtual machine as it is for any other Firebox or XTM device. One difference is that, for an XTMv virtual machine, you can connect to either the trusted interface or the external interface to run the Web Setup Wizard. If the external interface has been assigned an IP address, you can use that interface to connect to Fireware Web UI and run the Web Setup Wizard.

Note

If you do not complete the Web Setup Wizard within 15 minutes, the wizard does not save any of your settings. You must log in and start the wizard again.

The Web Setup Wizard includes a step to activate your XTMv device. At this step, you can choose from one of three activation options:

Online Activation
With *Online Activation*, the wizard activates your XTMv device and downloads the feature key to enable all the functionality for your XTMv device. If you have the device serial number, and the XTMv virtual machine has an Internet connection on the external interface, you can use online activation to allow the wizard to activate the device and automatically download a feature key.

Manual Activation
If you have already activated the XTMv device on the WatchGuard web site, and you have saved the feature key to a local file, you can select the *Manual Activation* option and paste the feature key into the wizard.

Skip Activation
f you do not have the serial number or feature key, you can choose the *Skip Activation* option and finish the wizard. This saves your other configuration settings and allows you to complete the wizard. If you skip activation, you must add the feature key later in Fireware Web UI or WatchGuard System Manager. Your device does not have full functionality until it has the feature key to enable the purchased feature set.

To set up the basic configuration file on an XTMv virtual machine:

1. Open a web browser and connect to Fireware Web UI on either the external or trusted interface.
   - **Connect to the external interface** — From any computer on the XTMv external network, connect to: `https://<External_IP_Address>:8080`
     For <External_IP_Address>, use the IP address you found in Step 4 of the previous procedure.
   - **Connect to the trusted interface** — From any computer on the XTMv trusted network, connect to: `https://10.0.1.1:8080`
2. Log in to Fireware Web UI with the default administrator account credentials.
   Username — `admin`
   Passphrase — `readwrite`
3. Click **Next**.
   The Web Setup Wizard Welcome page appears.
4. Select **Create a new device configuration** (the default option). Click **Next**.
   The license agreement appears.
5. Read the license agreement. You must accept the license agreement to continue. Click **Next**.
   The external interface configuration page appears.
6. Select the method to use to assign your XTMv device an external IP address:
   - **DHCP** — To use DHCP to assign the IP address, select this option. This is the default.
   - **PPPoE** — To use PPPoE to assign the IP address, select this option.
   - **Static** — To assign a static IP address, select this option.

7. Click **Next**.
8. *If you selected* **DHCP**, select **Obtain an IP automatically**, or **Use IP address** and type the IP address for the interface.

   If you selected **PPPoE**:

   - Select **Obtain an IP automatically**, or select **Use IP address** and type an IP address for the interface.
   - Type the PPPoE **User Name** and **Password**.

   If you selected **Static**, type the IP address for the external interface and type the IP address of the gateway.
9. Click **Next**.
   The Configure the DNS and WINS Servers page appears.
10. Type the **Domain Name** and the addresses of the **DNS Servers** and **WINS Servers** for the XTMv device to use. Click **Next**.
    The trusted interface configuration page appears.
11. Select an option for the trusted interface:
    - **IP Address** — Type the IP address to use for the trusted network interface (interface 1).
    - **DHCP Server** — Enables the DHCP server for the trusted interface. In the **From** and **To** text boxes, type the range of addresses the DHCP server can assign.

      When you select this option, the XTMv device is the DHCP server for devices that connect to the virtual network for the trusted interface. Do not enable the DHCP server on this interface if a DHCP server is already configured on the same network.
12. Click **Next**.
13. Type a passphrase for the **status** (read only) and **admin** (read/write) accounts on the XTMv device. Click **Next**.
14. Type the **Device Name** (required), **Device Location** (optional), and **Contact Person** (optional) for this XTMv device. Click **Next**.
15. Select the **Time Zone** where the XTMv device is located. Click **Next**.
    The Online Activation page appears.
16. Select an activation option:
    - If you have the serial number, but not the feature key, select **Use Online Activation** and provide this information:
      - **Device Name** — A name to identify this device in your account on the WatchGuard web site.
      - **Serial Number** — The XTMv serial number you received when you purchased the device — this is different from the default serial number that ends with 000000000, which is the serial number for an unactivated device.
      - **User Name** — The user name you use to log in to the WatchGuard web site.
      - **Password** — The password you use to log in to the WatchGuard web site.
    - If you already have the feature key, select **Skip Online Activation** and select **Add the feature key**. Copy and paste the text from the local feature key file in the text box.
    - If you do not have the serial number or feature key, select **Skip activation** and select **Skip this step**.
17. Click **Next**.
    The Summary page appears.
18. Review your settings. Click **Next** to apply the settings.
    The Setup is Complete page appears.

After the Setup Wizard Finishes

After you complete the Web Setup Wizard, the XTMv virtual machine is configured with a basic configuration that allows outbound TCP, UDP, and ping traffic, and blocks all unrequested external traffic, except management connections.

For an XTMv virtual machine, the default *WatchGuard* and *WatchGuard Web UI* policies allow management connections from any computer on the trusted, optional, or external networks. This is different from the default configuration for other WatchGuard devices, which do not allow management connections from the external network. If you do not want to allow management connections from the external network, edit these policies to remove the **Any-External** alias from the **From** list. To allow management from only a specific computer on the external network, you can add the address of that management computer to the **From** list in these policies.

You can use Fireware Web UI, WatchGuard System Manager, or the Fireware Command Line Interface (CLI) to change the configuration for your XTMv virtual machine. You can connect to either the trusted or external interface from any computer on the same network.

If you changed the IP address of the interface you used to connect to the Fireware Web Setup Wizard, you must use the new address to connect and manage the device.

Fireware Web UI

To connect to your XTMv virtual machine with Fireware Web UI:

1. Open a web browser and type `https://<interface_ip_address>:8080`.
   The Web UI login page appears.
2. From the **User Name** drop-down list, select **admin**.
3. In the **Passphrase** text box, type the admin passphrase you configured in the wizard.
4. Click **Login**.

For more information about how to manage your XTMv device with Fireware Web UI, see the *Fireware Help* at http://www.watchguard.com/help/documentation/.

WatchGuard System Manager

To manage your XTMv device with WatchGuard System Manager, you must install the WatchGuard System Manager software on a Windows computer located on the XTMv external, trusted, or optional network.

To connect to your XTMv virtual machine with WatchGuard System Manager:

1. In WatchGuard System Manager, select **File > Connect to Device**.
   The Connect to Firebox dialog box appears.
2. In the **Name / IP Address** text box, type the IP address of the XTMv interface you want to connect to.
3. Type the status passphrase you configured in the wizard.
4. Click **Login**.

For information about how to install WatchGuard System Manager and manage an XTMv device with WatchGuard System Manager, see the *Fireware Help* at http://www.watchguard.com/help/documentation/.

Fireware Command Line Interface (CLI)

You can manage your XTMv virtual machine with the Fireware CLI from the console in the vSphere Client, or you can connect through a serial port.

To use the CLI through a serial port, you must allocate a serial port to the XTMv virtual machine. You can use a physical serial port or connect over a network.

To use the CLI in the console:

1. In the **vSphere Client Inventory** tree, select the virtual device.
2. Select the **Summary** tab.
3. Click **Open Console**.
4. Log in with the **admin** or **status** account credentials and the passphrase you configured in the wizard.

For information about how to use the CLI to manage Fireware, see the *Command Line Interface Reference* on the Product Documentation page at http://www.watchguard.com/help/documentation/.

Reset an XTMv Virtual Machine to Factory Default Settings

If you want to run the Web Setup Wizard again for an XTMv virtual machine, you can use the Fireware CLI to reset the virtual machine to factory default settings.

To reset the XTMv virtual machine to factory default settings:

1. Log in to the CLI with the **admin** account.
2. Run the command `restore factory-default`.

ESXi Resource Allocation

To achieve the expected performance and scalability for your XTMv edition, we recommend that you allocate these resources to the XTMv virtual machine:

	Small Office Edition	Medium Office Edition	Large Office Edition	Datacenter Edition
Virtual CPUs	1	2	4	8 or more
Memory	1 GB	2 GB	4 GB	4 GB or more

You can also allocate additional network adapters, up to a total of 10, that correspond to interfaces 0–9 in the Fireware configuration.

Add Network Adapters

When you deployed the XTMv virtual appliance, you selected two networks to map to the default external and trusted XTMv network interfaces. To enable other network interfaces in the Fireware network configuration, you must add network adapters to the XTMv virtual machine. All XTMv editions support a maximum of 10 network adapters.

To add a network adapter:

1. Launch the vSphere Client and log in to the ESXi host with administrator credentials.
2. In the vSphere Inventory tree, right-click the virtual machine and select **Power > Power Off**.
3. Right-click the virtual machine, select **Edit Settings**.

4. On the **Hardware** tab, click **Add**.
5. Select **Ethernet Adapter** as the type of device to add. Click **Next**.
6. From the **Type** drop-down list, select **E1000**.
7. From the **Network label** drop-down list, select the name of the virtual network to add. Click **Next**.
8. Review the selected options. Click **Finish**.

To add another network adapter, repeat these steps. You can add a maximum of 10 network adapters.

Configure the Virtual Switch

To work correctly, these Fireware networking features require that you configure the virtual switch (vSwitch) on your network in promiscuous mode:

- Bridge mode network configuration
- Network/LAN bridge
- Mobile VPN with SSL with the **Routed VPN Traffic** setting
- FireCluster management interface

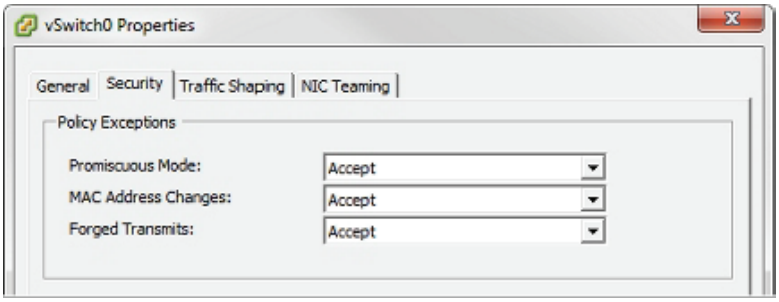
In the vSphere Client, you configure promiscuous mode in the vSwitch security properties.

To use multiple VLANs on a single interface on an XTMv device in an ESXi environment, configure the vSwitch for the XTMv VLAN interface to use VLAN ID 4095 (All).

vSwitch Configuration for FireCluster

To configure an active/passive FireCluster in an ESXi environment, you must enable promiscuous mode on the vSwitch that connects to the FireCluster management interface.

You must configure the vSwitch that connects to a FireCluster external interface to accept MAC address changes.



Configure Virtual Processors

By default, the XTMv virtual machine is allocated one virtual CPU. For optimal performance, configure the virtual machine to use the recommended number of CPUs for your XTMv edition.

To configure CPU resources:

1. Launch the vSphere Client and log in to the ESXi host with administrator credentials.
2. In the vSphere Inventory tree, right-click the virtual machine and select **Power > Power Off**.
3. Right-click the virtual machine, select **Edit Settings**.
4. From the **Hardware** list, select **CPUs**.
5. From the **Number of virtual processors** drop-down list, select the number of virtual processors recommended for your XTMv edition.

Configure Memory Resources

By default the XTMv virtual machine is allocated 1 GB of memory. For optimal performance, configure the virtual machine to use the recommended memory resources for your XTMv edition.

To configure memory resources:

1. Launch the vSphere Client and log in to the ESXi host with administrator credentials.
2. In the vSphere Inventory tree, right-click the virtual machine and select **Power > Power Off**.
3. Right-click the virtual machine and select **Edit Settings**.
4. In the **Hardware** list, select **Memory**.
5. In the **Memory Size** text box, type or select the memory size recommended for your XTMv edition.

FireCluster on VMware ESXi

You can configure two XTMv virtual machines as a FireCluster. We recommend that you complete the virtual network setup on the hypervisor before you configure the XTMv devices you want to cluster.

Plan the Cluster

Before you configure FireCluster, plan your network and configure the vSwitch for each interface.

Verify Basic Components

Make sure that you have these items:

- Two WatchGuard XTMv virtual machines of the same type (Small Office, Medium Office, Large Office or Datacenter Edition)
- The same version of Fireware on each device
- The feature key for each XTMv virtual machine
- One vSwitch configured for each cluster interface
- One vSwitch for each active traffic interface
- WatchGuard System Manager, to edit the FireCluster configuration

Plan Your Network

Before you enable FireCluster, we recommend you identify the vSwitch, network interface, and network addresses to use. For FireCluster, the external interface must use a static IP address. A clear plan helps you configure the interface IP addresses, and configure the vSwitch settings as required for each interface. For example, you could create a table that looks something like this:

	vSwitch name	XTMv device Interface #	IP address
Primary cluster interface	HA-net	9	Member 1: 10.10.5.1/24 Member 2: 10.10.5.2/24
Interface for management IP address	Trusted-net	1	Member 1: 10.10.1.2/24 Member 2: 10.10.1.3/24
External interface	External-net	0	203.0.113.2 /24
Trusted interface	Trusted-net	1	10.10.1.1/24

Configure Network Switches

You must configure a vSwitch for each interface you want to enable. We recommend you do this before you enable FireCluster. Before you enable FireCluster, make sure that the switches are configured to meet these requirements:

- The vSwitch for the external interface must be configured to accept MAC address changes
- The vSwitch for the FireCluster management interface must have promiscuous mode enabled
- The vSwitch that connects to each cluster interface must be dedicated to this purpose

For more information about switch configuration, see "Configure the Virtual Switch" on page 16.

Configure the Cluster

After you have planned your network and configured the vSwitches, you can set up the XTMv virtual machines and enable FireCluster.

Deploy and Provision two XTMv Virtual Machines

To create a FireCluster with two new XTMv virtual machines, use the procedure in the previous section to deploy and activate two XTMv devices. If you want to enable FireCluster for an existing XTMv virtual machine, deploy and activate one additional XTMv virtual machine. For more information, see "XTMv Installation" on page 6.

Allocate the same resources (network adapters, virtual CPU, and memory) to each XTMv virtual machine. For more information, see "ESXi Resource Allocation" on page 15.

Get the Feature Key for the Second Device

Copy the feature key from the second device to a text file, so that you can add it to the FireCluster configuration.

To copy the feature key with Policy Manager:

1. In WatchGuard System Manager, connect to the XTMv virtual machine that will be the second device in the cluster.
2. Select **Tools > Policy Manager**.
3. Select **Setup > Feature Keys > Details**.
4. Select and copy the feature key details to a text file.

Configure FireCluster

The steps to configure FireCluster on XTMv are the same as for any other XTM device, except that you must select active/passive for an XTMv FireCluster.

To configure the FireCluster:

1. In WatchGuard System Manager, connect to the XTMv virtual machine that has the configuration you want to use for the cluster.
2. Select **Tools > Policy Manager**.
3. Select **FireCluster > Setup**.
   The FireCluster Setup Wizard starts.
4. Click **Next**.
5. Select **Active/Passive cluster**.
   Even though you can select it, the Active/Active cluster option is not supported for XTMv.

6. Select the **Cluster ID**.
   The cluster ID uniquely identifies the cluster if you set up more than one cluster on the same layer 2 broadcast domain. If you have only one cluster, you can use the default value of 1.
7. Click **Next**.
8. Select a **Primary** cluster interface.
   Select an interface that is connected to a dedicated vSwitch. The cluster interface is dedicated to communication between cluster members and is not used for other network traffic.
9. (Optional) Select a **Backup** cluster interface.
   If you select a backup cluster interface, select an interface connected to a second dedicated vSwitch.
10. Select the **Interface for management IP address**.

    You use this interface to connect directly to FireCluster member devices for maintenance operations. The cluster master also uses the Management IP address of the backup master to communicate with the backup master about device status and action aggregation.

    This is not a dedicated interface. It also is used for other network traffic. You cannot select a VLAN interface as the Interface for Management IP address.We recommend that you select the interface that the management computer usually connects to.

Note

Make sure that promiscuous mode is enabled on the vSwitch for the interface you configure as the Interface for management IP address.

11. Click **Next**.
12. When prompted by the configuration wizard, add these FireCluster member properties for each device:

    Feature Key
    For each device, add the feature key to get the device serial numbers and to enable all features. For the first cluster member, the wizard automatically uses the feature key that exists in the configuration file.

    Member Name
    The name that identifies each device in the FireCluster configuration.

    Primary cluster interface IP address
    The IP address the cluster members use to communicate with each other over the primary cluster interface. The primary cluster interface IP address for each cluster member must be an IPv4 address on the same subnet.

    If both devices start at the same time, the cluster member with the highest IP address assigned to the primary cluster interface becomes the master.

    Backup cluster interface IP address
    (Optional) The IP address the cluster members use to communicate with each other over the backup cluster interface. The backup cluster interface IP address for each cluster member must be an IPv4 address on the same subnet.

Note

Do not set the Primary or Backup cluster IP address to the default IP address of any interface on the device. The default interface IP addresses are in the range 10.0.0.1 - 10.0.17.1. The Primary and Backup cluster IP addresses must not be used for anything else on your network, such as virtual IP addresses for Mobile VPN, and the IP addresses used by remote branch office networks.

Management IP address

A unique IP address that you can use to connect to an individual XTM device while it is configured as part of a cluster. You must specify a different management IP address for each cluster member. If the interface you chose as the Interface for management IP address has IPv6 enabled, you can optionally configure an IPv6 management IP address.

The IPv4 management IP address can be any unused IP address. We recommend that you use an IP address on the same subnet as the interface you select as the Interface for management IP address. This is to make sure that the address is routable. The management IP address must be on the same subnet as the WatchGuard Log Server or syslog server that your FireCluster sends log messages to.

The IPv6 management IP address must be an unused IP address. We recommend that you use an IPv6 address with the same prefix as an IPv6address assigned to the interface you selected as the Interface for management IP address. This is to make sure that the IPv6 address is routable.

13. Review the configuration summary on the final screen of the FireCluster Setup Wizard. The configuration summary shows the options you selected and which interfaces are monitored for link status.
14. Click **Finish**.
    The FireCluster Configuration dialog box appears.

Form the Cluster

To form the cluster, save the configuration file to each XTMv virtual machine.

1. In Policy Manager, select **File > Save > To Firebox** to save the configuration to the original XTMv virtual machine.
2. In Policy Manager, select **File > Save > To Firebox** again, and specify the IP address of the second XTMv virtual machine.

   Policy Manager displays a warning if the IP address that you save the configuration to does not exist in the configuration file. Since you want to replace the existing configuration, click **Yes** to confirm that you want to save the file.

The cluster forms automatically. To verify whether a cluster has formed, connect to the device in WatchGuard System Manager and refresh the status periodically. If the cluster does not form automatically after a few minutes, reboot or power cycle each virtual machine to trigger automatic cluster formation.

Other ESXi Configuration Options

The options in this section are only necessary for specific Fireware features.

USB Drive

To use a USB drive for system backup and restore, you must connect the USB drive to the server where your ESXi host is installed. Then you must add the USB device to the XTMv virtual machine. You can add a USB drive to only one virtual device at a time.

To add a USB drive to your XTMv device:

1. Connect a USB drive to the server where your ESXi host is installed.
2. Launch the vSphere Client and log in to the ESXi host with administrator credentials.
3. In the vSphere Inventory tree, right-click the XTMv virtual machine and select **Edit Settings**.
4. On the **Hardware** tab, click **Add**.
5. Select **USB device** as the device type. Click **Next**.
6. Select the connected USB device. Click **Next**.
7. Click **Finish**.

Serial Port

You can connect to the Fireware CLI over a serial port, if you add a serial port to the XTMv virtual machine configuration. The serial port can use a physical serial port on the host, or you can connect through a network.

To add a virtual serial port to your XTMv virtual machine:

1. Launch the vSphere Client and log in to the ESXi host with administrator credentials.
2. In the vSphere Inventory tree, right-click the virtual machine and select **Power > Power Off**.
3. Right-click the virtual machine and select **Edit Settings**.
4. On the **Hardware** tab, click **Add**.
5. Select **Serial Port** as the device type. Click **Next**.
6. Select **Connect via Network**. Click **Next**.
7. In the **Network Backing** section, select **Server**.
8. In the **Network Backing** section, in the **Port URI** text box, type `telnet://:<IP address>:<port>`
   - `<IP address>` is the management IP address of your ESXi host.
   - `<port>` is an unused port on the ESXi host.

   For example, if the ESXi server management IP address is 10.10.10.10, and you want to use port 3344 for the virtual serial port, type `telnet://:10.10.10.10:3344`
9. In the **Device Status** section, make sure the **Connect at power on** check box is selected.
10. Click **Finish**.
11. Power on the XTMv virtual machine.

To connect to the XTMv virtual serial port:

1. From a computer that can reach the ESXi server over the network, use the telnet client to connect to the configured IP address and port.
   For example, `telnet 10.10.10.10 3344`
2. Log in with the XTMv virtual machine **admin** or **status** account and passphrase.

For information about how to use the CLI to manage your XTMv device, see the *Command Line Interface Reference* on the Product Documentation page at http://www.watchguard.com/help/documentation/.

IPv6

To enable IPv6 on an XTMv virtual machine network interface, you must enable IPv6 on the network adapter on the ESXi host.

For information about IPv6 configuration in Fireware, see the *Fireware Help* at http://www.watchguard.com/help/documentation/.

XTMv Setup on Microsoft Hyper-V

This chapter describes how to deploy and configure an XTMv virtual machine on Microsoft Windows Server 2012 with a Hyper-V role. The installation steps are similar for other Hyper-V environments.

Installation Prerequisites

You must install the XTMv virtual device in a Microsoft Hyper-V environment that meets these requirements:

- **Hyper-V**
  - To install an XTMv virtual device, you must install the Hyper-V role on Windows Server 2008 R2 or Windows Server 2012.
  - The procedures in this document use the Hyper-V Manager on Windows Server 2012 to deploy, configure, and provision the XTMv virtual machine in the Hyper-V environment. You can also use System Center Virtual Machine Manager (VMM) interface, or a Hyper-V role on a client computer instead of Hyper-V Manager.
  - Make sure your Windows Server or Hyper-V Server software is updated to the latest patch level.
- **Hardware**
  - The hardware requirements for XTMv are the same as the hardware requirements for Hyper-V on Windows Server 2008 R2 or Windows Server 2012.
  - Each XTMv virtual machine requires 3 GB of disk space.

XTMv Installation

Before You Begin

To prepare for your installation, make sure you have these things:

- Hyper-V installed on Windows Server 2008 R2, Windows Server 2012, Hyper-V Server 2008 R2, or Hyper-V Server 2012.
- XTMv device serial number.
  You receive the serial number when you purchase the XTMv virtual device.
- WatchGuard XTMv virtual hard disk (.vhd) file
  The file name is xtmv_<version>.vhd, where <version> is the Fireware version.
- *(optional)* WatchGuard System Manager v11.7.3 or higher

Download the XTMv zip file for Hyper-V and the WatchGuard System Manager software from the from the *Software Downloads* page on the WatchGuard website.

Extract the .vhd file from the .zip file to a location on the Windows server where Hyper-V is installed. You might want to extract the .vhd file to the default location where Hyper-V stores virtual hard disks. On Windows Server 2012, the default location is `C:\Users\Public\Public Documents\Hyper-V\Virtual hard disks`.

Note

Because a .vhd file is a virtual hard drive, it cannot be used for more than one powered on virtual machine at the same time. To deploy additional XTMv virtual machines, make sure that you save a copy of the unzipped .vhd file with a unique name for each virtual machine. Then, when you add the virtual machine, make sure you select the .vhd file to use with that virtual machine.

Installation Overview

To complete initial installation, perform these procedures as described in the subsequent sections:

1. Create the XTMv virtual machine and select the .vhd file to use.
2. Assign network adapters, and power on the XTMv virtual machine.
3. Connect to the XTMv virtual machine and run the Web Setup Wizard to set up a basic configuration.
4. Allocate additional resources to the XTMv virtual machine.

This guide describes how to use the Web Setup Wizard to create your initial configuration. If you have installed WatchGuard System Manager on a computer on the XTMv device trusted network, instead of the Web Setup Wizard, you can use the Quick Setup Wizard in WatchGuard System Manager to discover the XTMv virtual machine and set up the basic device configuration.

Note

To activate your device in the Web Setup Wizard, you must have the device serial number. You cannot use a serial number that ends with 000000000, which is the serial number for an unactivated device.

Network Considerations

When you create the XTMv virtual appliance, it is initially configured with two active interfaces.

External interface
The external interface, Interface 0, is set up by default to request an IP address from a DHCP server. To connect to this interface for the initial device configuration, you must map this interface to a destination network that has a DHCP server.

Trusted interface
The trusted interface, Interface 1, has a default IP address of 10.0.1.1.

When you create the XTMv virtual machine in the Hyper-V environment, before you run the Web Setup Wizard for the XTMv device, you must add at least two network adapters (not legacy network adapters) to the virtual machine for the external and trusted interfaces.

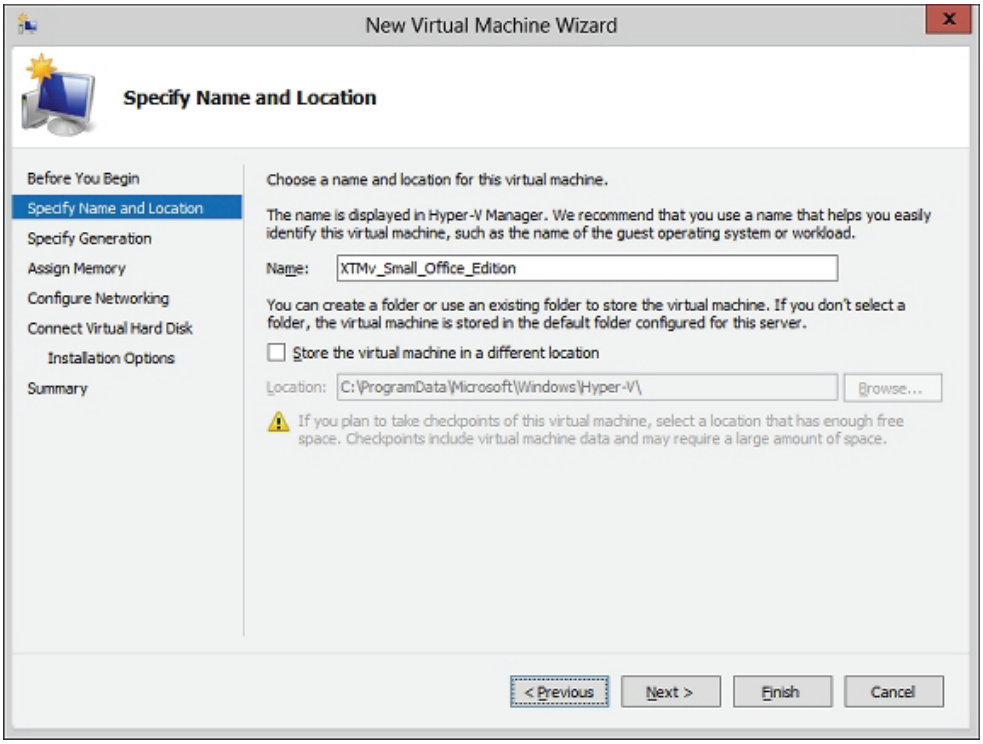
After you create the XTMv virtual machine, you can enable and configure additional XTMv network interfaces. For additional interfaces to operate, you must configure the XTMv virtual machine in the Hyper-V Manager or System Center VMM to add the number of network adapters you want to enable in the XTMv configuration.

Create the XTMv Virtual Machine

You can use the Hyper-V Manager or System Center VMM to create the XTMv virtual machine.

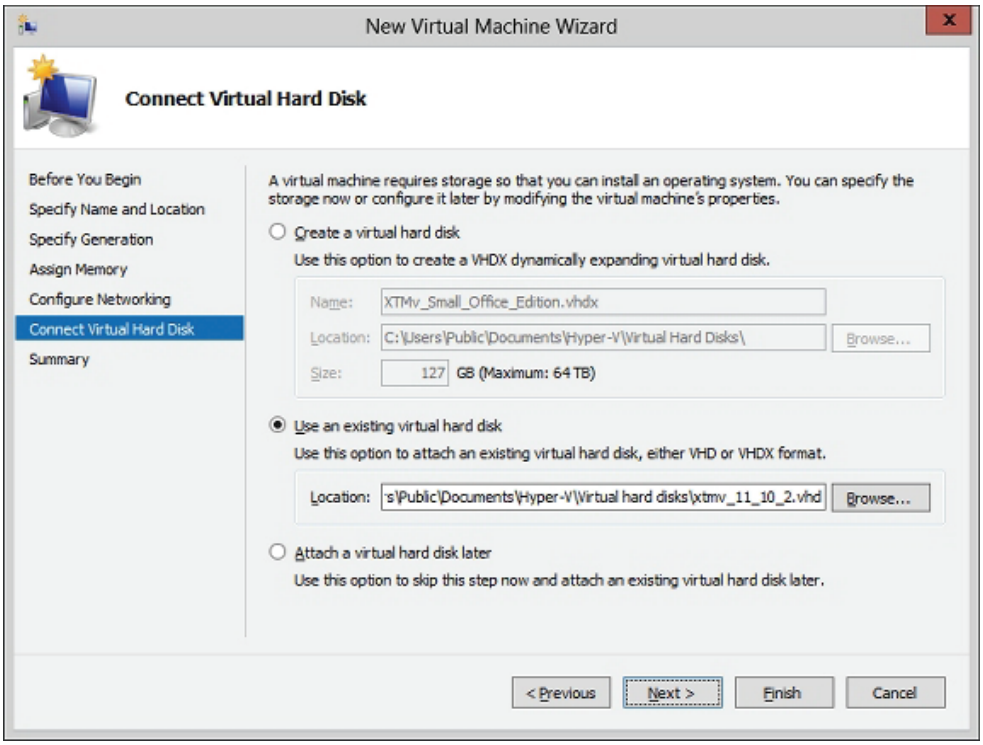
To use the Hyper-V Manager:

1. On your Windows 2008 R2 Server or Windows 2012 Server, launch Hyper-V Manager.
2. Select **Action** > **New > Virtual Machine**.
   The New Virtual Machine Wizard starts.
3. If the **Before You Begin** page appears, click **Next**.
   The Specify Name and Location page appears.

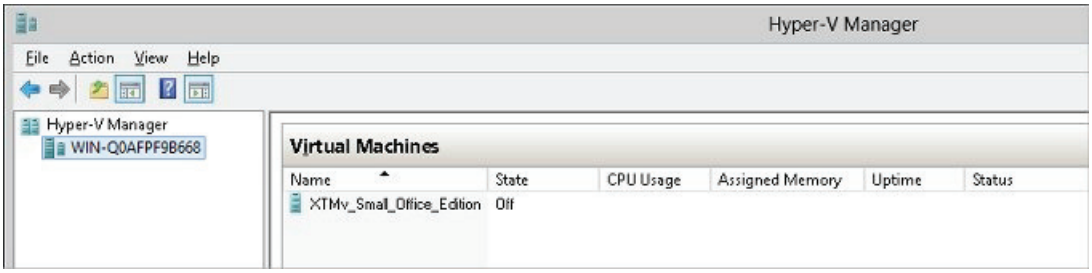


4. In the **Name** text box, type a name for this virtual machine.

5. To store the virtual machine in a folder other than the default folder, select the **Store the virtual machine in a different location** check box. Click **Browse** and select the location to store the virtual machine. Click **Next**.
   For Hyper-V 2012, the Specify Generation page appears. For Hyper-V 2008, the Assign Memory page appears.
6. On the **Specify Generation** page, select **Generation 1**. Click **Next**.
7. In the **Startup memory** text box, type the amount of memory to allocate based on your XTMv edition:
   - Small Office Edition — 1024 MB
   - Medium Office Edition — 2048 MB
   - Large Office or Datacenter Edition — 4096 MB
8. Click **Next**.
   The Configure Networking page appears.
9. From the **Connection** drop-down list, select the virtual network adapter to use for the external interface, Eth0. Do not choose a legacy network adapter.
10. Click **Next**.
    The Connect Virtual Hard Disk page appears.



11. Select **Use an existing virtual hard disk**.
12. Click **Browse** and select the location where you saved the WatchGuard XTMv .vhd file. Click **Next**.
13. Review the summary. Click **Finish**.
    The XTMv virtual machine appears in the Hyper-V Manager Virtual Machines pane.



Add Network Adapters

Before you can configure Fireware on your XTMv virtual machine, you must add two virtual network adapters to it. The first one you select is for the external interface, Eth0. The second one is for the trusted interface, Eth1. The virtual network adapters you use for your XTMv device must be a network adapter, not a legacy network adapter.

In the New Virtual Machine Wizard, you selected the first virtual network adapter. Next, you must add the virtual network adapter to use for the XTMv virtual machine trusted interface, Eth1. You must do this while the virtual machine is not started.

1. In the **Virtual Machines** pane, select the XTMv virtual machine you just added.
2. From the **Actions** list, select **Settings**.
3. From the **Hardware** list, select **Add Hardware**.
4. Select **Network Adapter** and click **Add**.
   Do not select Legacy Network Adapter. XTMv does not support legacy network adapters.
5. From the **Virtual switch** drop-down list, select the virtual switch to use for the XTMv device trusted interface (Eth1). Click **Apply**.
6. Verify that both network adapters appear in the **Hardware** list. Click **OK**.

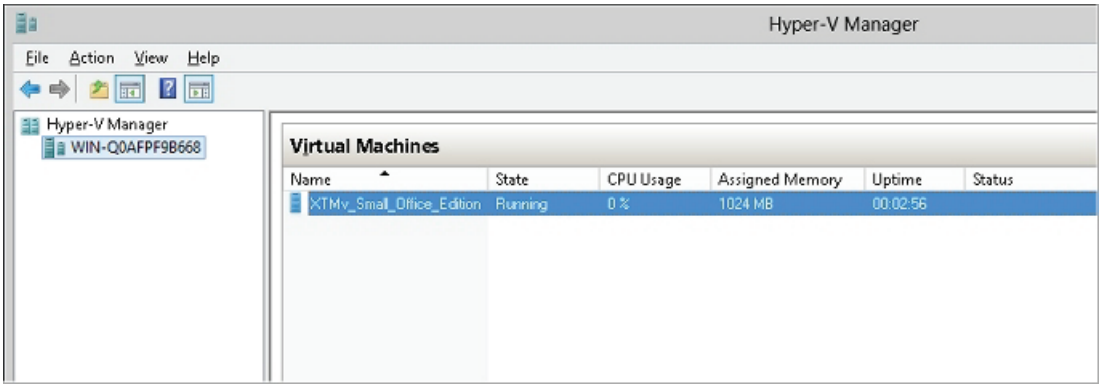
If you know what additional resources you want to allocate to this virtual machine, you can allocate those resources now, before you start the virtual machine. Or, you can complete this step later. For more information about how to allocate additional resources, see "Hyper-V Resource Allocation" on page 33.

Start the XTMv Virtual Machine

Next, you start the XTMv virtual machine. When you initially power on the XTMv virtual machine, it automatically sends a DHCP broadcast to request an IP address for the external interface. If a DHCP server is configured on the external network, the XTMv external interface receives an IP address.

To power on the XTMv virtual machine:

1. In the Hyper-V Manager **Virtual Machines** pane, select the virtual machine.
2. From the **Actions** list, click **Start**.
   Or, select **Action > Start**.
   The XTMv virtual machine is powered on with factory default settings. The device state is Running.



XTMv Factory Default Settings

When you power on the XTMv virtual machine for the first time, it starts with these factory default settings:

- The XTMv device has two active interfaces: external and trusted.
- The trusted interface has the IP address 10.0.1.1.
- The external interface is configured to receive an IP address through DHCP.
- The trusted interface is not configured to assign IP addresses with DHCP.
  This is different than the default setting for other XTM devices.
- Both the trusted and external interfaces accept management connections.
  This is different than the default setting for other XTM devices.
- The **admin** account passphrase is `readwrite`.
- The serial number for an unactivated XTMv device ends with 000000000.
  You assign the actual serial number during device activation.

Find the External IP Address

If the external network has a DHCP server, the XTMv device external interface is automatically assigned an IP address. If you want to use this IP address to connect to the device, you can use the Fireware Command Line Interface to see what IP address has been assigned to the external interface.

To use the CLI to see the IP addresses assigned to an active XTMv device:

1. In the **Virtual Machines** pane, select the XTMv virtual machine.
2. From the **Actions** list, select **Connect**.
3. At the login prompt, type `status`.
4. At the password prompt, type `readonly`.
   This is the default status account passphrase.
5. Type `show interface`.
   The command output shows the IP addresses and status for the External and Trusted interfaces.

```
WG>show interface
--
-- Interface Properties
-- Type:  TR = trusted, EX = external, OP = optional, VL = vlan, BR = bridge, CL
 = cluster,LA = <link aggregation, NA = not apply
--
physical interface count : 2
licensed interface count : 2
--
-- Interface Address & Status
--
Enabled If-#  Name                    Address    Type/MTU  Status IP-Assignment
IP-Mode-Type
 yes    0    External          203.0.113.120/24 EX/1500   up     static        I
Pv4 Only
 yes    1    Trusted               10.0.1.1/24 TR/1500   up     static        I
Pv4 Only
WG>_
```

6. To log out of the Fireware CLI, type `exit`.

For more information about how to manage an XTMv device with the Fireware CLI, see the *Command Line Interface Reference* at http://www.watchguard.com/help/documentation/.

Use the Web Setup Wizard to Create a Basic Configuration

The Fireware Web Setup Wizard is almost the same for an XTMv virtual machine as it is for any other Firebox or XTM device. One difference is that, for an XTMv virtual machine, you can connect to either the trusted interface or the external interface to run the Web Setup Wizard.

Note

If you do not complete all of the Web Setup Wizard steps within 15 minutes, the wizard does not save any of your settings. You must log in and start again.

The Web Setup Wizard includes a step to activate your XTMv device. At this step, you can choose from one of three activation options:

Online Activation
With *Online Activation*, the wizard activates your XTMv device and downloads the feature key to enable all the functionality for your XTMv device. If you have the device serial number, and the XTMv virtual machine has an Internet connection on the external interface, you can use online activation to allow the wizard to activate the device and automatically download a feature key.

Manual Activation
If you have already activated the XTMv device on the WatchGuard web site, and you have saved the feature key to a local file, you can select the *Manual Activation* option and paste the feature key into the wizard.

Skip Activation
f you do not have the serial number or feature key, you can choose the *Skip Activation* option and finish the wizard. This saves your other configuration settings and allows you to complete the wizard. If you skip activation, you must add the feature key later in Fireware Web UI or WatchGuard System Manager. Your device does not have full functionality until it has the feature key to enable the purchased feature set.

To set up the basic configuration on an XTMv virtual machine:

1. Open a web browser and connect to Fireware Web UI on either the external or trusted interface.
   - **Connect to the external interface** — From any computer on the XTMv external network, connect to: `https://<External_IP_Address>:8080`
     For <External_IP_Address>, use the IP address you found in Step 4 of the previous procedure.
   - **Connect to the trusted interface** — From any computer on the XTMv trusted network, connect to: `https://10.0.1.1:8080`

Note

You can use the web browser on the Windows Server to connect to one of these addresses, if you have installed Flash in the browser.

2. Log in to Fireware Web UI with the default administrator account credentials.
   Username — `admin`
   Passphrase — `readwrite`
3. Click **Next**.
   The Web Setup Wizard Welcome page appears.
4. Select **Create a new device configuration** (default). Click **Next**.
   The license agreement appears.
5. Read the license agreement. You must accept the license agreement to continue. Click **Next**.
   The external interface configuration page appears.
6. Select the method to use to assign your XTMv device an external IP address:

- **DHCP** — To use DHCP to assign the IP address, select this option. This is the default.
- **PPPoE** — To use PPPoE to assign the IP address, select this option.
- **Static** — To assign a static IP address, select this option.

7. Click **Next**.
8. If you selected **DHCP**, select **Obtain an IP automatically**, or select **Use IP address** and type the IP address for the interface.

   If you selected **PPPoE**:

   - Select **Obtain an IP automatically**, or select **Use IP address** and type an IP address for the interface.
   - Type the PPPoE **User Name** and **Password**.

   If you selected **Static**, type the IP address for the external interface and type the IP address of the gateway.
9. Click **Next**.
   The Configure the DNS and WINS Servers page appears.
10. Type the **Domain Name** and the addresses of the **DNS Servers** and **WINS Servers** for the XTMv device to use. Click **Next**.
    The trusted interface configuration page appears.
11. Select an option for the trusted interface:
    - **IP Address** — Type the IP address to use for the trusted network interface (interface 1).
    - **DHCP Server** — Enables the DHCP server for the trusted interface. In the **From** and **To** text boxes, type the range of addresses the DHCP server can assign.

      When you select this option, the XTMv device is the DHCP server for devices that connect to the virtual network for the trusted interface. Do not enable the DHCP server on this interface if a DHCP server is already configured on the same network.
12. Click **Next**.
13. Type a passphrase for the **status** (read only) and **admin** (read/write) accounts on the XTMv device. Click **Next**.
14. Type the **Device Name** (required), **Device Location** (optional), and **Contact Person** (optional) for this XTMv device. Click **Next**.
15. Select the **Time Zone** where the XTMv device is located. Click **Next**.
    The Online Activation page appears.
16. Select an activation option:
    - If you have the serial number, but not the feature key, select **Use Online Activation** and provide this information:
      - **Device Name** — A name to identify this device in your account on the WatchGuard web site.
      - **Serial Number** — The XTMv serial number you received when you purchased the device — this is different from the default serial number that ends with 000000000, which is the serial number for an unactivated device.
      - **User Name** — The user name you use to log in to the WatchGuard web site.
      - **Password** — The password you use to log in to the WatchGuard web site.
    - If you already have the feature key, select **Skip Online Activation** and select **Add the feature key**. Copy and paste the text from the local feature key file in the text box.
    - If you do not have the serial number or feature key, select **Skip activation** and select **Skip this step**.
17. Click **Next**.
    The Summary page appears.
18. Review your settings. Click **Next** to apply the settings.
    The Setup is Complete page appears.

After the Setup Wizard Finishes

After you complete the Web Setup Wizard, the XTMv virtual machine is configured with a basic configuration that allows outbound TCP, UDP, and ping traffic, and blocks all unrequested external traffic, except management connections.

For an XTMv virtual machine, the default *WatchGuard* and *WatchGuard Web UI* policies allow management connections from any computer on the trusted, optional, or external networks. This is different from the default configuration for other WatchGuard devices, which do not allow management connections from the external network by default. If you do not want to allow management connections from the external network, edit the *WatchGuard* and *WatchGuard Web UI* policies to remove the **Any-External** alias from the **From** list. To allow management from only a specific computer on the external network, you can add the address of that management computer to the **From** list in these policies.

You can use Fireware Web UI, WatchGuard System Manager, or the Fireware Command Line Interface (CLI) to change the configuration for your XTMv virtual machine. You can connect to either the trusted or external interface from any computer on the same network.

If you changed the IP address of the interface you used to connect to the Fireware Web Setup Wizard, you must use the new address to connect and manage the device.

Fireware Web UI

To connect to your XTMv virtual machine with Fireware Web UI:

1. Open a web browser and type `https://<interface_ip_address>:8080`.
   The Fireware Web UI login page appears.
2. From the **User Name** drop-down list, select **admin**.
3. In the **Passphrase** text box, type the admin passphrase you configured in the wizard.
4. Click **Login**.

For more information about how to manage your XTMv device with Fireware Web UI, see the *Fireware Help* at http://www.watchguard.com/help/documentation/.

WatchGuard System Manager

To manage your XTMv device with WatchGuard System Manager, you must install the WatchGuard System Manager software on a Windows computer located on the XTMv external, trusted, or optional network.

To connect to your XTMv virtual machine with WatchGuard System Manager:

1. In WatchGuard System Manager, select **File > Connect to Device**.
   The Connect to Firebox dialog box appears.
2. In the **Name / IP Address** text box, type the IP address of the XTMv interface you want to connect to.
3. Type the status passphrase you configured in the wizard.
4. Click **Login**.

For information about how to install WatchGuard System Manager and manage an XTM device with WatchGuard System Manager, see the *Fireware Help* at http://www.watchguard.com/help/documentation/.

Fireware Command Line Interface (CLI)

You can manage your XTMv virtual machine with the Fireware CLI when you connect to the virtual machine in Hyper-V Manager or over a serial port.

To use the CLI through a serial port, you must allocate a serial port to the XTMv virtual machine. You can use a physical serial port or connect over a network.

To use the CLI in the Hyper-V MAnager:

1. In Hyper-V Manager, in the **Virtual Machines** pane, right-click the XTMv virtual machine.
2. Select **Connect**.
3. Log in with the **admin** or **status** account credentials and the passphrase you configured in the wizard.

For information about how to use the CLI to manage Fireware, see the *Command Line Interface Reference* on the Product Documentation page at http://www.watchguard.com/help/documentation/.

Reset an XTMv Virtual Machine to Factory Default Settings

If you want to run the Web Setup Wizard again for an XTMv virtual machine, you can use the Fireware CLI to reset the virtual machine to factory default settings.

To reset the XTMv virtual machine to factory default settings:

1. Log in to the CLI with the **admin** account.
2. Run the command `restore factory-default`.

Hyper-V Resource Allocation

To achieve the expected performance and scalability for your XTMv edition, we recommend that you allocate these resources to the XTMv virtual machine:

	Small Office Edition	Medium Office Edition	Large Office Edition	Datacenter Edition
Virtual CPUs	1	2	4	8 or more
Memory	1 GB	2 GB	4 GB	4 GB or more

You can also allocate additional network adapters, up to a total of 10, that correspond to interfaces 0–9 in the Fireware configuration.

Add Network Adapters

Before you ran the Web Setup Wizard to configure the XTMv virtual machine, you added two virtual network adapters for the default external and trusted XTMv network interfaces. Before you enable other network interfaces in the Fireware network configuration, you must add network adapters to the XTMv virtual machine.

Note

You must add adapters to the XTMv device in Hyper-V before the adapters are configurable on the XTMv device. For example, if you add only two virtual adapters to the XTMv device, the Fireware UI shows only two configurable interfaces for that device.

All XTMv editions support a maximum of 10 interfaces, but, because you cannot use legacy network adapters with an XTMv virtual machine, the practical limit for XTMv in a Hyper-V environment is eight.

Hyper-V supports two types of virtual network adapters:

- Network adapters (Hyper-V supports a maximum of eight)
- Legacy network adapters (Hyper-V supports a maximum of four); Do not use legacy network adapters with XTMv.

To add a network adapter in Hyper-V Manager:

1. In the **Virtual Machines** pane, select the XTMv virtual machine.
2. Right-click the virtual machine and select **Turn Off**.
3. Right-click the virtual machine and select **Settings**.
4. From the **Hardware** list, select **Add Hardware**.
5. Select **Network Adapter** and click **Add**.
6. From the **Virtual switch** drop-down list, select a virtual network adapter.

To add another network adapter, repeat these steps. You can add a maximum of eight network adapters.

Add Virtual Processors

By default, the XTMv virtual machine is allocated one virtual CPU. For optimal performance, configure the virtual machine to use the recommended number of CPUs for your XTMv edition.

To add a network adapter in Hyper-V Manager:

1. In the **Virtual Machines** pane, select the XTMv virtual machine.
2. Right-click the virtual machine and select **Turn Off**.
3. Right-click the virtual machine and select **Settings**.
4. From the **Hardware** list, select **Processor**.
5. In the **Number of virtual processors** text box, type or select the number of processors recommended for your XTMv edition.

Configure Memory Resources

For optimal performance, configure the virtual machine to use the recommended memory resources for your XTMv edition. You configured the memory resources when you created the virtual machine.

To configure memory resources for an existing virtual machine:

1. In the **Virtual Machines** pane, select the XTMv virtual machine.
2. Right-click the virtual machine and select **Turn Off**.
3. Right-click the virtual machine and select **Settings**.
4. From the **Hardware** list, select **Memory**.
5. In the **Startup RAM** text box, type the memory size recommended for your XTMv edition.