

WatchGuard Firebox[®] Vclass QuickStart Guide

Thank you for purchasing the WatchGuard Firebox Vclass. The Firebox Vclass acts as a barrier between your networks and the public Internet, protecting them from security threats.

This QuickStart Guide covers the initial installation of the WatchGuard Firebox Vclass. Please refer to the accompanying user documentation for comprehensive instructions and hardware specifications.

1. Check Package Contents

Your package should contain the following:

- WatchGuard Firebox Vclass security appliance
- This QuickStart Guide
- User Documentation
- WatchGuard Firebox Vcontroller CD-ROM
- Power cable
- Ethernet, serial, optical data, and/or appliance-to-UPS cables based on the Firebox Vclass appliance you purchased. See the *Installation Guide* for more information on which cables are available for your Firebox Vclass model.

2. Gathering Network Information

You should gather the following network information needed during the quick setup process.

Firebox Vclass Serial Number

Found on the back of your Firebox Vclass under the barcode.

Network Addresses

Default Gateway:

Subnet Mask:

Public Interface:

Private Interface:

3. Cabling the Firebox

The first step in cabling your WatchGuard Firebox Vclass is to determine its location based on what you intend to protect. A Firebox Vclass can be used to protect one portion of your company's network from unauthorized internal users or to protect your entire network from external threats on the Internet.

After you determine where to place the appliance within your network infrastructure, physically place the appliance where it has access to a network hub or router.

- 1 Remove the Firebox Vclass appliance from its packaging.
- 2 Place the appliance on any stable flat surface near the Management Workstation and a network hub or router.
- 3 Use a tan straight-through Ethernet cable or optical cable to connect the Firebox Private interface (0) to the network hub or router.
- 4 Use a tan straight-through Ethernet or optical cable to connect the Firebox Public interface (1) to your public network.

NOTE: The v60[®] and v80[®] appliances have a DMZ or Firebox Mixed-Access interface (2). Use a tan straight-through Ethernet or optical cable to connect the Firebox Mixed-Access interface (2) to your mixed-access network.

- 5 Plug the power cord into the Firebox power input and into a power source. For the v10 model, this connection powers on the appliance. For the v60 and v80, press the power switch on the back of the appliance to power on the appliance.
If connecting the appliance to a UPS device, use the power cable supplied with the security appliance to connect the two devices through their respective RS-232 ports.

4. Setting Up the Management Station

You can administer the WatchGuard Firebox Vclass from any computer that you designate as the Management Station. The following instructions are for Windows. See the *Installation Guide* for instructions for other operating systems.

To designate the Management Station, install the Vcontroller software as follows:

- 1 Insert the WatchGuard Firebox Vcontroller CD-ROM. Locate and double-click the CD-ROM drive icon. Double-click the Windows folder. Double-click setup.exe.
- 2 Follow the onscreen instructions to install the Vcontroller management software.
If prompted to install a new version of the Java Development Kit (JDK), you can either choose to install the Vcontroller version over any existing JDK or skip this part of the installation.
- 3 At the end of the install, you will be prompted to start the Vcontroller. Click **Yes**.
The Vcontroller window appears followed by the Login dialog box.

NOTE: You must activate your LiveSecurity Service to enable VPN 3DES encryption or receive WatchGuard Support. To activate your LiveSecurity Service, go to:
<http://www.watchguard.com/activate>
For more information on activating the LiveSecurity Service, see the *Policy Configuration Guide*, Chapter 2, Service and Support.

5. Using Device Discovery to Identify the Firebox

Use WatchGuard Vcontroller to discover a new factory-default Firebox Vclass security appliance on your network and assign the new unit a permanent, static IP address. The Firebox should be connected to the same LAN segment or subnet as your Management Workstation through the Private interface (0).

- 1 When the Login dialog box first appears, click the binoculars icon.
- 2 Click **Find** to start the discovery process.
If the Management Station has more than one network interface card, use the pop-up menu to select the IP address of the appropriate card before proceeding.
- 3 A status box appears and remains open until the discovery process is complete.
When a discovery has been made, the Devices Found window appears. See the *Installation Guide* to troubleshoot a failed discovery.
- 4 Select the serial number of the Firebox Vclass you are currently setting up.
- 5 Click **Set Interface 0 IP**.

- 6 Enter the IP address assigned to the Firebox Vclass Private (0) interface.
- 7 Enter the subnet mask for the local network on which the Firebox Vclass resides.
- 8 Click **Update**.
- 9 Click **Apply All**. Click **Yes** to confirm the Interface 0 IP.
- 10 Record any information in the Result window not already taken down and click **Close**.
The Firebox automatically reboots. Once the restart sequence is complete, you can use the Vcontroller Login dialog box to connect to the Firebox and start the configuration process.

6. Configuring the Firebox

The Vcontroller Installation Wizard configures a newly discovered Firebox Vclass with a basic configuration while simultaneously updating the Vcontroller management software for use with this and other Firebox Vclass appliances.

NOTE: Use the Vcontroller Installation Wizard after you successfully complete the Device Discovery process.

- 1 Use the Vcontroller Login dialog box to connect to the Firebox using the IP address or domain name representing the new unit. Type **admin** in both the Login and Password fields, then click **OK** to proceed.
The Installation Wizard Welcome window appears.
- 2 Click **Next** to proceed with configuration. Enter the following General information:

System Name	Identify the Firebox by a name of your choosing. This is a required field. Example: SeattleFirewall
System Location	Brief description of where the Firebox will be located or used such as a building or floor number. Example: LANRoom
System Contact:	Name and contact information of the principal system administrator or department responsible for maintenance of the Firebox. Example: jay_le@company.com
System Time	Set Firebox date, time, and time zone. Click Change to configure.
- 3 Click **Next** to continue. Enter the Private interface information:

IP Address	Enter the private, trusted IP address.
Network Mask	Enter the network mask of the private IP address, usually 255.255.255.0.
- 4 Select Static, DHCP, or PPPoE to define how the Firebox receives its public, external IP address. Selecting an option results in fields appearing to configure that option. Complete the addressing fields.
For example, when you select Static, fields appear prompting for the IP address and network mask.
- 5 Click **Next** to proceed. Click **Save Only**. Click **OK**.
If you select Apply, the Firebox will reboot immediately with the information entered thus far.
- 6 If you want, you can configure routing at this time. To configure a default gateway, enter the public (interface 0) IP address in the Specify Default Route field. To configure additional routes, click **Add** and complete the Add Route dialog box. For more information on configuring routes, see the

Installation Guide. When you complete adding routes, click **Next** and then **OK**.

- 7 If you want, you can configure a DNS server at this time. You must provide the Firebox domain name and insert the IP addresses of any DNS servers. Click **Next** to continue.
- 8 If you want, you can automatically implement default firewall policies.
We recommend that you review the defaults against the security policy preferences of your organization. For more information, see the *Installation Guide*. For example, you might want to deselect Allow Ping to the Device to prevent internal "Ping of Death" exploits.

7. Deploying the Firebox into Your Network

The Firebox can now be used as a basic firewall. If you have not already done so, you should now deploy the Firebox in its permanent network location.

- Complete a software shutdown of the Firebox.
Launch Vcontroller and connect to the Firebox using the Firebox name or IP and the system administrator password. From the main Vcontroller window, select **Shut Down**. Click **OK**.
- Place the Firebox in its permanent location.
- Connect the Firebox to your network and a power source.
- Change the default gateway setting on all desktops to the Firebox Trusted interface IP address.

8. What's Next?

Congratulations! You have successfully installed, configured, and deployed your new Firebox Vclass security appliance on your network. What's next? Here are some things to remember as a new customer:

Customizing your security policy

You customize your security policy by adding traffic actions that expand what you allow in and out of your firewall. Every action brings trade-offs between network security and accessibility. When selecting actions, balance the needs of your organization with the requirement that the computer assets be protected from attack.

Please refer to the *Policy Configuration Guide* and *System Administration Guide* for more information and assistance on configuring traffic actions.

What to expect from your LiveSecurity Service

Your Firebox includes a 3-month subscription to our award-winning LiveSecurity Service. Your subscription:

- Enables 3DES encryption and/or High Availability.
- Provides up-to-date network protection with the latest software upgrades.
- Solves problems with comprehensive technical support resources including known issues and Frequently Asked Questions.
- Reduces downtime with alerts and configuration tips to combat the newest threats and vulnerabilities.
- Keeps you prepared for upcoming security threats with editorials and analysis from industry experts.
- Extends your network security with bundled software, utilities, and special offers.