
WatchGuard High Availability Guide

The WatchGuard High Availability option enables the installation of two Fireboxes on one network in a fail-over configuration. At any given moment, one Firebox is in active mode while the other is in standby mode. The standby Firebox activates when the first Firebox goes offline. Once a Firebox becomes active, it stays active until it is taken offline and the other Firebox becomes primary again. Both Fireboxes in a High Availability installation must have identical configuration files.

What is High Availability?

In a High Availability configuration, the two Fireboxes take turns using a single IP address. One Firebox becomes the primary unit and assumes the IP address while the other becomes the standby. The primary/standby relationship is dynamic: The first Firebox to reboot becomes the primary Firebox. If they boot up simultaneously the two Fireboxes negotiate primary and standby status. When the primary Firebox first boots, it brings up the standby Firebox, which then runs without an IP address.

If a Firebox detects another Firebox in active mode but detects no standby, that Firebox goes into standby mode. It brings up the network

standby interface and adds a route to the fail-over network. It then makes a connection to the primary event processor, starts the control channel, and monitors the active Firebox.

The Fail-Over Process

The standby Firebox constantly monitors the active Firebox. When it no longer detects the active Firebox, the standby Firebox switches to active mode. When this happens the fail-over program first kills the control channel (firewalld will start its own later) and makes sure that the event processor connection is properly set up. It then allows the init program to boot the previously active Firebox.

When fail-over occurs and the standby box switches to active mode, it immediately begins using the last configuration file it received.

At this point, the standby Firebox checks to see if its configuration file differs from the active Firebox. Since it cannot determine which configuration file is right, however, it only logs that it detected a difference.

The configuration file is identical on both machines. To put a new configuration file onto the fail-over cluster, the Management Station must have network access to both the active and standby Fireboxes.

Monitoring Firebox Health

A critical part of High Availability is that the Fireboxes monitor each other constantly for their levels of functionality. Checking for ARP packets determines if an IP address is taken, but doesn't verify that the active Firebox is healthy. ARP responses are handled at a very low level. For example, Firebox proxies could die while the kernel continued to run. High Availability checks to see if the active Firebox control channel is working. If the active Firebox cannot receive a TCP connection via port 4105, the standby Firebox needs to reboot and take over.

Rebooting

The need for a reboot is communicated with a reboot packet. The reboot packet is a UDP packet destined for port 4105 on the Firebox fail-over IP address. It contains a checksum of the Firebox's cookie as well as other identifying information. It is shared via a broadcast UDP packet as soon

in the boot process as possible. The reboot packet is broadcast when it sees an ARP request that matches certain settings.

The fail-over daemon listens for reboot packets. If it encounters a packet containing the reboot command and has the proper cookie checksum, the target Firebox is immediately rebooted.

Installing High Availability

High Availability requires that you first install two Fireboxes on the Trusted interface between the router and trusted network. Then download and install the High Availability software, and run the QuickSetup Wizard again to configure the primary Firebox for High Availability.

Preparing your Network for High Availability

Prepare for installation according to the heading that best describes your situation:

Adding a Second Firebox to a Functioning Installation

- If your second Firebox has the WatchGuard LiveSecurity System 4.1 or later installed on its flash memory, use the network connection to configure the Fireboxes via TCP/IP instead of the direct-connect serial cable.
- If your second Firebox has not been initiated with the LiveSecurity System 4.1 software, connect it to the Management Station with a serial cable and run the QuickSetup Wizard to initialize it. Then install it on the Trusted interface.

Refer to the *Install Guide* for instructions on installing and configuring a Firebox.

Creating a Brand New High Availability Installation with Two Fireboxes

- If both Fireboxes are packaged with WatchGuard LiveSecurity System 4.1 or later software, use a network connection to configure the Fireboxes via TCP/IP.
- If either Firebox is packaged with LSS 4.0 or a previous version of the WatchGuard software, connect that Firebox to the Management Sta-

tion with a serial cable and run the QuickSetup Wizard to initialize it. Disconnect the Firebox you just initialized from the serial cable, and attach the second Firebox. Run QuickSetup Wizard a second time. Install both initialized Fireboxes on the Trusted Interface.

Refer to the *Install Guide* for instructions on installing and configuring a Firebox.

Downloading the High Availability Software

The WatchGuard High Availability module includes these instructions as well as a license key. Register your license key and then download the High Availability software from the WatchGuard LiveSecurity Archive.

Registering High Availability

1. Open your Web browser to the LiveSecurity archive at:
<http://www.watchguard.com/archive/>
2. Log in to the LiveSecurity Archive.
3. Click Register High Availability Now.
4. Enter your High Availability license key including the hyphens.
The most common reason for registration to fail is incorrectly typing the numbers and hyphens of the License Key.
5. Click Register.
The High Availability license key is associated with your LiveSecurity license to ensure that you receive regular updates to the High Availability utility. The download page opens.
6. Click Download.
A prompt appears to open or save the High Availability installation file. The file name is `WGInstallHA.wls`.
7. Save the file to your Windows desktop.

High Availability Installation Procedure

1. On your Windows desktop, double-click **WGInstallHA.wls**.
The WatchGuard Player appears.
2. Click Install.
The WinZip Self-Extractor appears.
3. Click Setup.
The installation wizard starts.
4. Enter your High Availability license key. Click Next.
The installation wizard enables High Availability in the QuickSetup Wizard.

5. Click OK.

The installation program installs the High Availability software in the proper directories. You still must configure High Availability for your security policy, which is described in the next section.

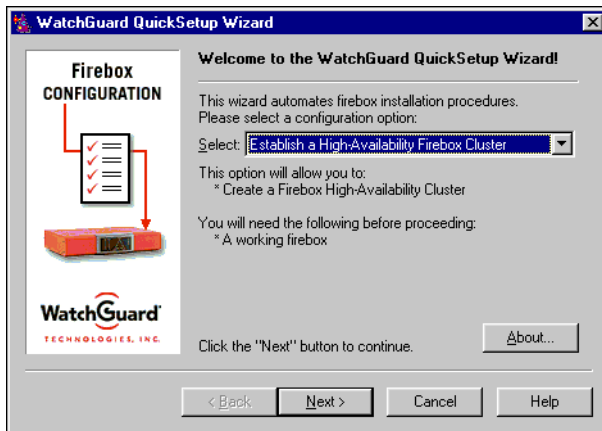
Configuring High Availability



- The optional High Availability module must be downloaded and installed on the Management Station.
- Both Fireboxes must be initialized with the LiveSecurity System 4.1 or later software. Recently built Fireboxes are shipped preconfigured from the factory with LSS 4.10.
- Both Fireboxes should be installed on the Trusted interface, ready to be configured.
- Identify the active Firebox (the one configured and currently protecting the network) and the standby Firebox (the one being added to implement High Availability).

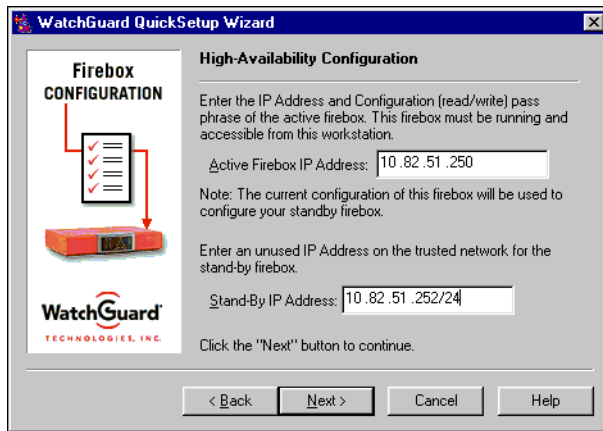
1. Select Start ⇒ Programs ⇒ WatchGuard ⇒ QuickSetup Wizard.

The Quick Setup Wizard appears.



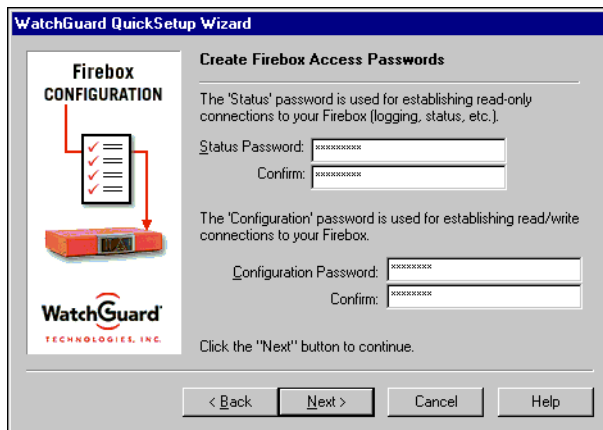
2. Use the Configuration Option dropdown list to select Establish a High-Availability Firebox Cluster. Click Next.

The High Availability Configuration screen appears.



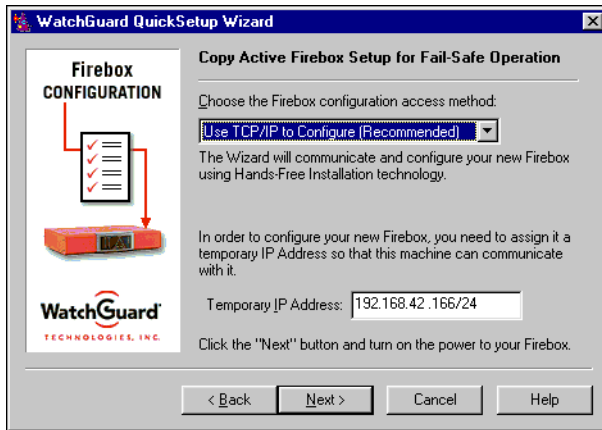
3. Enter the Trusted IP address of the currently active Firebox in the Active Firebox IP Address field.
4. Enter an unused IP address in the Stand-By IP Address field. Click Next.

The Enter Active Firebox Passwords screen appears.



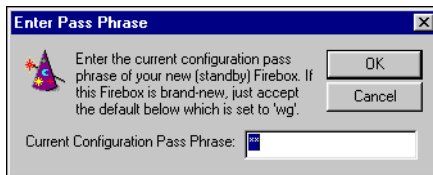
5. Enter and confirm the active Firebox read-only password in the Status Password and first Confirm fields.
6. Enter and confirm the active Firebox read-write password in the Configuration Password and second Confirm fields.
7. Press Next.

The Copy Active Firebox Setup for Fail-safe Operation screen appears.



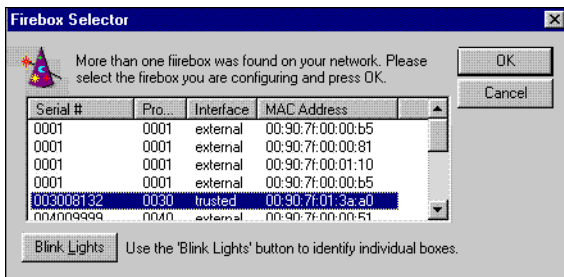
8. Connect both Fireboxes the Ethernet via TCP/IP. Use the Access Method drop list to select Use TCP/IP to Configure (Recommended).
9. Enter or view the temporary IP address for the new standby Firebox. Click Next.

The Enter Pass Phrase dialog box appears.



10. Enter or accept the Current Configuration Pass Phrase (this is the read-write password for the standby Firebox). If this is a new Firebox, accept the default password, **wg**. Click OK.
11. Turn on the standby Firebox when prompted by the Wizard.

The Firebox Selector dialog box displays.



12. Select the standby Firebox from the Firebox Selector list.

If you are unsure which serial number corresponds to which Firebox on your network click the Blink Lights button. It causes the highlighted Firebox's front panel lights to blink and flash.

13. When you have selected the standby Firebox, click OK.

High Availability copies the configuration file from your primary Firebox and uploads it to the standby Firebox. Then both Fireboxes reboot. The first box to finish rebooting becomes the primary Firebox until it is shut off or fails.

The active Firebox front panel lights up to indicate the flow of traffic through the Firebox. The standby Firebox indicates standby mode by alternately blinking the SysA and SysB lights on its front panel.

14. [Optional] You can test the High Availability mechanism by turning off the active Firebox.

Within a minute the standby Firebox boots into active mode. When you turn the other Firebox back on, it goes into standby mode.

Troubleshooting High Availability

If the second Firebox does not respond to the new configuration, you may need to upload the LiveSecurity System 4.1 version to the Firebox flash disk memory. To do so:

1. Connect the second Firebox directly to the Management Station with the serial cable as described in the *Install Guide*.
2. Perform the full Firebox initialization procedure where you start with an unpowered Firebox and turn it on to flash its memory when prompted to do so by the QuickSetup Wizard. See the *Install Guide*.
3. Place the second Firebox on the network next to the first Firebox on the Trusted Interface.
4. Run the QuickSetup Wizard to configure High Availability as described in "Installing High Availability" on page 3.

Copyright and Patent Information

Copyright© 1998 - 2000 WatchGuard Technologies, Inc. All rights reserved.

WatchGuard, Firebox, and LiveSecurity are either a trademark or registered trademark of WatchGuard Technologies, Inc. in the United States and other countries. This product is covered by one or more pending patent applications.

DocVer S-1.0-HighAvailability-3