

# WatchGuard® High Availability Guide

---

High Availability for WatchGuard System Manager



---

## **Notice to Users**

---

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

## **Copyright, Trademark, and Patent Information**

---

Copyright© 1998 - 2004 WatchGuard Technologies, Inc. All rights reserved.

Complete copyright, trademark, patent, and licensing information can be found in the *WatchGuard System Manager User Guide*.

All trademarks or trade names mentioned herein, if any, are the property of their respective owners.

WFS Software Number v7.2

# Contents

---

The High Availability Failover Process .....	1
Installing High Availability .....	3
Connecting Fireboxes in a High Availability cluster .....	5
Configuring High Availability .....	5
<i>Configuring High Availability with the wizard</i> .....	6
<i>Configuring High Availability manually</i> .....	7



---

# WatchGuard® High Availability Guide

---

The High Availability upgrade enables the installation of two Fireboxes on one network in a failover configuration with one Firebox in active mode and the other in standby mode. The standby Firebox activates when the active Firebox goes offline. After a Firebox becomes active, it stays active until it is taken offline and the standby Firebox resumes as the active unit. Both Fireboxes in a High Availability cluster must have the same configuration file. High Availability is easy to set up and ensures system stability.

---

## NOTE

---

The term "Firebox" refers to either the Firebox III or the Firebox X unless specifically stated. Illustrations of Fireboxes are interchangeable unless specifically stated.

---

## The High Availability Failover Process

---

To create a High Availability cluster, you need two Fireboxes that are the same model. One is designated as the active Firebox and the other is designated as the standby Firebox. The active/standby relationship is dynamic: The first Firebox to reboot becomes the active Firebox. If they boot simultaneously, the two Fireboxes negotiate active and standby status.

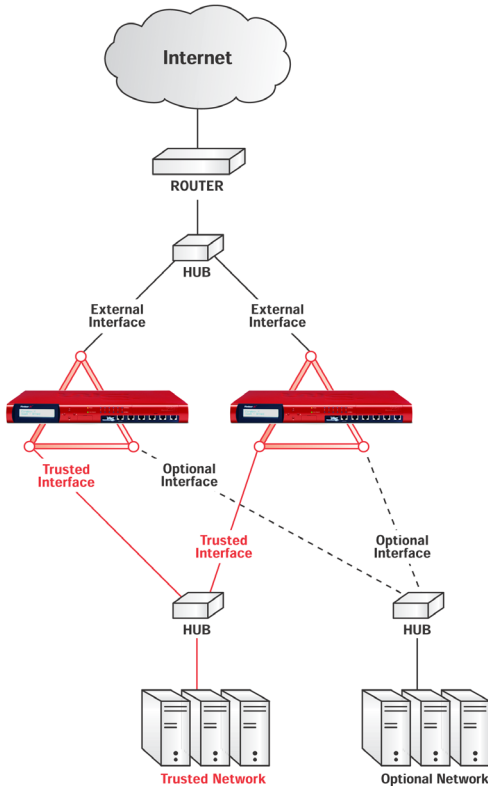
---

### NOTE

If both Fireboxes are active and connected to the network, one of the Fireboxes will reboot in standby mode. This is called High Availability stand down.

---

Both Fireboxes must be connected to your network in the same way. For example, both external interfaces should be connected to the same hub or switch. The following figure shows a network with a High Availability configuration.



You can configure the High Availability connection between the two Fireboxes on any Firebox interface, but the default connection is on the trusted interface. The standby Firebox needs to have its own reserved IP address on the same subnet as the interface with High Availability enabled. This allows the active and standby Fireboxes to exchange two types of data:

- ARP packets or heartbeats
- TCP connection state information

The standby Firebox sends out ARP packets on the network every five seconds requesting the MAC address of the active Firebox. The active Firebox will respond with its MAC address. If the standby Firebox misses two of these ARP responses in a row, it assumes the active Firebox is offline and switches to active mode running with the last TCP connection state information it was sent by the offline Firebox.

The TCP connection state information contains the most recent information about the TCP connections on the active Firebox. The standby Firebox requests the TCP connection state information from the active Firebox, and the active Firebox sends this data over the TCP port 4105.

Both the active and standby Firebox must have the same configuration. To put a new configuration file onto the High Availability cluster, the management station must have network access to both the active and standby Fireboxes.

---

**NOTE**

The management station's IP address needs to be on the same subnet as the interface with High Availability enabled so that the management station can communicate with the High Availability cluster.

---

If you want to change the configuration file used in a High Availability cluster, you need to save the configuration file to the management station first. If you try to load a configuration file directly from a public folder on a share drive, the configuration file will only load on the active Firebox.

---

## Installing High Availability

---

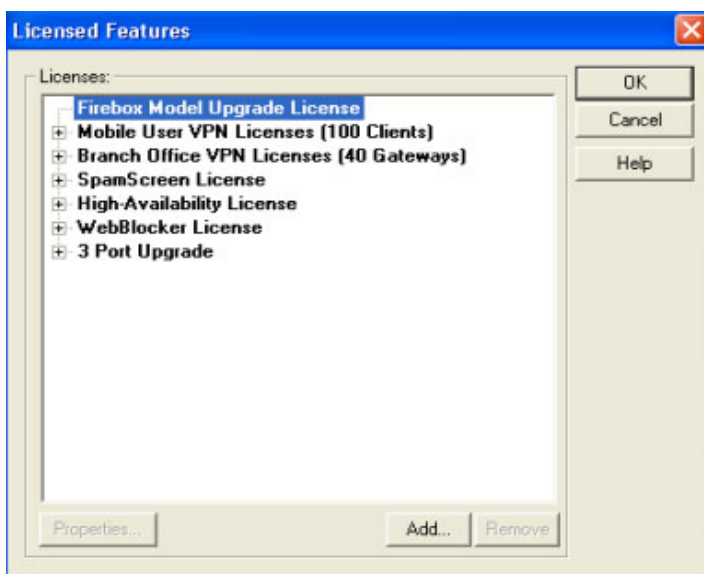
When you purchase and activate the High Availability upgrade key, you receive a license key. You have to add a separate High Availability license key to each Firebox in the High Availability cluster. You also need to have the same upgrades installed on each Firebox, so you need to add any upgrade keys installed on the active Firebox to the standby Firebox.

---

The Firebox X has a specific installation procedure because all Firebox X license keys are bound to its serial number. You need to add all the upgrade license keys for both the active and standby Firebox X to the configuration file because whichever Firebox X is active needs to read the keys that correspond to its serial number. Thus, for any given upgrade feature, the configuration file will contain two license keys, one corresponding to each serial number in the cluster. The presence of the standby Firebox X license keys does not cause any problems; a Firebox X will simply ignore any feature keys that does not match its serial number. Please see the LiveSecurity site for instructions on obtaining the necessary feature keys.

To enable High Availability, you must add the High Availability license keys for each Firebox to the **Licensed Features** dialog box.

- 1 From Policy Manager, select **Setup** ⇒ **Licensed Features**.  
The Licensed Features dialog box appears.



- 2 Click **Add**.  
The Add/Import License Keys dialog box appears.

- 3 In the **Add/Import License Keys** dialog box, either type your license keys or click **Browse** and find it on your network. Click **OK**.  
The High availability license now appears on the Licensed Features dialog box and High Availability is activated.

## Connecting Fireboxes in a High Availability cluster

---

How you connect the active and standby Fireboxes in a High Availability cluster depends on what scenario best describes your situation:

### **Adding a standby Firebox to a functioning Firebox installation**

- If your standby Firebox has the Firebox System Manager v7.2 or later installed, use the network connection to configure the Fireboxes by way of TCP/IP.
- If your standby Firebox has not been initiated with Firebox System Manager v7.2 or later software, connect it to the management station with a serial cable and run the QuickSetup Wizard to initialize it. Then install it on the interface with High Availability enabled. The default is the trusted interface.

Refer to the “Firebox Read-Only System Area” section of the Reference Guide for instructions on installing and configuring a Firebox using a serial cable.

### **Creating a new High Availability installation with two uninstalled Fireboxes**

- If both Fireboxes are packaged with WatchGuard System Manager v7.2 or later, use a network connection to configure the Fireboxes via TCP/IP.

## Configuring High Availability

---

Before configuring your Fireboxes for High Availability, check the following:

- The two Fireboxes must be identical models.

- 
- The connection between the two Fireboxes should be configured on one of the Firebox interface.
  - Identify the active Firebox (configured and currently protecting the network) and the standby Firebox (being added to implement High Availability).

You can configure High Availability by either using the wizard or manually. The wizard connects the two Fireboxes on the trusted interface. You can select any interface when you configure High Availability manually.

## Configuring High Availability with the wizard

- 1 Select **Start** ⇒ **Programs** ⇒ **WatchGuard** ⇒ **QuickSetup Wizard**.  
The QuickSetup Wizard appears.
- 2 Click **Establish a High-Availability Firebox Cluster** from the drop-down list. Click **Next**.  
The High Availability Configuration screen appears.
- 3 Enter the IP address of the current active Firebox in the **Active Firebox IP Address** field.
- 4 In the **Stand-By IP Address** field, enter an unused IP address from the same subnet as the interface with High Availability enabled. The default is the trusted interface. Click **Next**.  
The Enter Active Firebox Passwords screen appears.
- 5 Enter and confirm the active Firebox read-only password in the **Status Passphrase** and **Retype Passphrase** fields.
- 6 Enter and confirm the active Firebox read/write password in the **Configuration Passphrase** and **Retype Passphrase** fields.
- 7 Click **Next**.  
The Copy Active Firebox Setup for Fail-safe Operation screen appears.
- 8 Click the method, TCP/IP or Serial, used to connect the Fireboxes from the drop-down list.  
It is recommended to use TCP/IP (Hands-Free). If you use Serial, you will need to select the serial port from the drop-down list.
- 9 Enter the temporary IP address for the new standby Firebox. This should be the same IP address that you entered earlier as the Stand-by IP address.

10 Click **Next**.

If you selected TCP/IP as the connection method, the Enter Pass Phrase dialog box appears. If you selected Serial as the connection method, the Enter Pass Phrase dialog box does not appear.

11 (TCP/IP connection only) 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**.

12 Turn on the standby Firebox when prompted by the Wizard. The QuickSetup Wizard identifies the Fireboxes and requests the High Availability license keys. After entering the license keys, the standby Firebox boots into standby mode.

---

**NOTE**

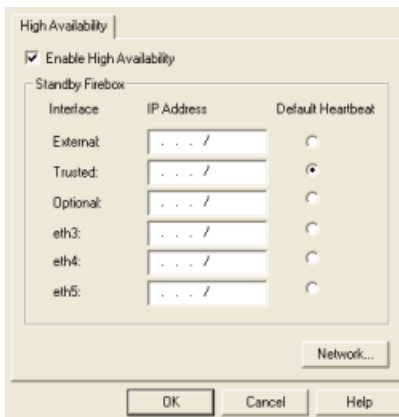
Remember that both of the Fireboxes now have separate IP addresses. You must not put any other TCP/IP devices on the network that have either of these addresses or the communication between the two Fireboxes may be interrupted causing unintentional High Availability failover.

---

## Configuring High Availability manually

After adding the High Availability license keys, you will set up the standby Firebox:

- 1 From Policy Manager, select **Network** ⇒ **High Availability**. The High Availability dialog box appears as shown below. You do not see eth3, eth4 and eth5 if you have a Firebox III.



- 
- 2 Select the **Enable High Availability** checkbox.  
The Standby Firebox fields activate.
  - 3 Select the **Default Heartbeat** checkbox for the interface you want to enable High Availability. The default is the trusted interface.
  - 4 In the **IP Address** field next to the selected **Default Heartbeat**, enter an unused IP address from the same subnet as the interface with High Availability enabled on the active Firebox. This will become the permanent IP address of the standby Firebox.  
It is important that no other devices ever use this IP address or the communication between the active and standby Fireboxes can be interrupted.
  - 5 Click **OK**.
  - 6 Save this configuration to the active Firebox.
  - 7 Close Policy Manager.
  - 8 Connect the blue serial cable that came with one of the Fireboxes to COM1 of the management station computer and to the Console port of the standby firebox.
  - 9 From Firebox System Manager, click **Main Menu button** ⇒ **Tools** ⇒ **Advanced** ⇒ **Flash Disk Management**.
  - 10 Click **Boot from the System Area (Factory Default)** and click **Continue**.  
You will be warned that the operation requires a serial cable, click Yes.
  - 11 You will be prompted for an IP address. Enter the same IP address you entered earlier in High Availability dialog box. This should be the same IP address that you entered earlier as the Stand-by IP address.
  - 12 Click **OK**.
  - 13 Select the COM port that the blue serial cable is connected to on your configuration workstation.
  - 14 Click **OK**.  
The Flash Disk Management tool will reset the Firebox and assign the temporary IP address that you specified.  
When the operation is complete, open the Policy Manager with your current configuration.
  - 15 Click **File** ⇒ **Save** ⇒ **To Firebox**.

- 16 Enter the temporary IP address that you just entered into the Flash Disk Management tool in this window.
- 17 Enter the password **wg**. This is the default factory password.
- 18 You will be prompted to save a new flash image and select passphrases. Configure the new Firebox with the exact same configuration and status passphrase that you used on the old Firebox.
- 19 When the operation is complete, the new Firebox will reboot and go into standby mode.

To test High Availability, turn off the active Firebox. Within 15 seconds, the standby Firebox will become active, resuming all packet filter connections that were in progress before the active Firebox went offline. Then, turn on the Firebox that is off. It will boot into the standby mode.

