
LiveSecurity System Install Guide

We appreciate your purchase of the WatchGuard LiveSecurity System. The WatchGuard LiveSecurity System consists of a suite of management and security software tools coupled with a plug-and-play network appliance called the WatchGuard Firebox. LiveSecurity is specifically designed to guard critical corporate or organizational assets from a continually changing barrage of threats.

The LiveSecurity System by its nature requires interdependence among distributed software, downloadable software, your Firebox, and the computer you use to administer the Firebox (the Management Station). This document walks you through these interdependent steps so your installation goes smoothly and you understand what is downloaded, expanded, installed, and configured.

Documentation

All WatchGuard LiveSecurity System documentation is stored on the LiveSecurity Installation CD-ROM in the Documentation directory. You also have the option to install the documentation on your local hard drive during installation. The documents are in the form of PDF files. You must have a copy of the Acrobat Adobe Reader® to read and print these files. Hard copies of the *Release Notes*, *Install Guide* and *User Guide* are included with the purchase of a Firebox.

Description of Technical Publications

Release Notes

Read these first to learn about known issues and new features since our prior release.

Internet Security Handbook

If you are a relative newcomer to the field of network security, read our security concepts primer. Learn more about Internet security and how our product, the LiveSecurity System, addresses the principal threats to your network.

Install Guide

This guide takes you step-by-step through downloading the LiveSecurity Service, installing the LiveSecurity Control Center, and using the QuickSetup Wizard to create an initial security policy configuration.

User Guide

The *User Guide* steps through the many features of the LiveSecurity Control Center and Security Suite software. It includes sections on how to use LiveSecurity services, configure and administer a security policy, and implement virtual private networking.

Reference Guide

A supplement to the *User Guide*, the *Reference Guide* provides additional material used to configure services and features such as detailed information about the IP protocol and a glossary of terms.

RUVPN Client Brochures

WatchGuard supports two forms of remote user virtual private networking: PPTP and IPSec. For your convenience, WatchGuard includes an end-user brochure for each RUVPN type.

Notational Conventions

WatchGuard manuals use the following notational conventions:

- When you select a menu command from a cascading menu, the command names are separated by an arrow (⇒) but with no special or separate font. For example, if the text says to: Select File ⇒Open, this means you should click the File menu and then click the Open command.
- Web site addresses display in a sans-serif font. For example:
`http://www.watchguard.com`
- Code and directory entries display in a sans-serif font. For example:
`[watchguard installation directory]\RUVPN\Exp`

Before You Install

Terms You Should Know

There are a few terms that are commonly used by WatchGuard when referring to our product and how it is implemented.

- **Management Station** — The computer on which you install and run the WatchGuard LiveSecurity Control Center software.
- **Event Processor** — The computer which receives and stores log messages and issues notifications. You can configure the Management Station to also serve as the event processor.
- **LiveSecurity Service** — The broadcast network that transmits security alerts, editorials, threat responses, and software updates directly to your desktop.
- **Trusted network** — The network behind the firewall which must be protected from the security challenge.
- **External network** — The network presenting the security challenge, typically the Internet.
- **Optional network** — A network protected by the firewall which communicates with both the Trusted and the External networks. Typically, the Optional network is used for “public” servers such as an FTP or Web server.
- **Drop In Configuration** — A drop-in network configuration is useful for situations where you can distribute your network’s logical address space across the Firebox’s interfaces. In a drop-in configuration, you place the Firebox physically between the router and the LAN, without re-configuring any of the machines on the Trusted interface.
- **Routed Configuration** — A routed network configuration is for situations where the Firebox is put in place with separate logical networks on its interfaces. It assigns separate network addresses to at least two of the three Firebox interfaces.
- **Secondary Network** — A secondary network is a network on the same physical wire as a Firebox interface which has an address belonging to an entirely different network.

Selecting Computers

- **Choose the computer you will use for the Management Station.**
The Management Station operating system platform must be Windows 95, Windows 98 or Windows NT (Service Pack 4 or 5).
- **Choose the computer you will use for the LiveSecurity Service. Verify that it has access to the Internet via Microsoft Internet Explorer® 4.0 (or later) or Netscape Communicator® 4.5 (or later).**
WatchGuard recommends that you use the Management Station as the computer for the LiveSecurity Service. However, if your configuration requires it you can designate an alternate computer.
- **Choose the computer you will use for the primary event processor.**
The primary event processor can be either the Management Station or another computer.

Minimum Requirements

This section describes the minimum hardware and software configurations necessary to successfully install, run, and administer version 4.1 of the WatchGuard LiveSecurity System.

Software Requirements

WatchGuard LiveSecurity System 4.1 can run on Microsoft Windows 95, Windows 98, or Windows NT 4.0 as specified below:

Windows 95 Requirements

- Microsoft Windows 95
- Service Release 2 or higher

Windows 98 Requirements

- Microsoft Windows 98

Windows NT Requirements

- Microsoft Windows NT 4.0
- Microsoft Service Pack 4 or Service Pack 5 for Windows NT 4.0

Web Browser Requirements

You need an HTML-based browser to use the online help included with the WatchGuard LiveSecurity System. These browsers and versions have proved to provide reliable, consistent display of WatchGuard Online Help:

- Netscape Communicator® 4.5 or later
- Microsoft Internet Explorer® 4.x

-
-
- Microsoft Internet Explorer® 5.01 or later

Hardware Requirements

Hardware requirements at a minimum are the same as for the operating system on which WatchGuard LiveSecurity System 4.1 runs. The recommended hardware ranges are listed below:

Table 1. WatchGuard LSS 4.1 Hardware Requirements

Hardware Feature	Minimum Requirement
CPU	Pentium
Memory	Same as for OS; Recommended: 32MB for Windows 95a 64MB for Windows 98 64 MB for Windows NT 4.1
Hard Disk Space	25 MB to install all WatchGuard modules 15 MB minimum for log file Additional space as required for log files Additional space as required for multiple configuration files
CD-ROM Drives	One CD-ROM drive to install WatchGuard from its CD-ROM distribution disk

Before Upgrading to 4.1 from Previous Versions

1. Make a copy of your current Firebox configuration file.
2. Exit and disable the WatchGuard Event Processor.
3. Uninstall any previous versions of WatchGuard software.

Installing the LiveSecurity System

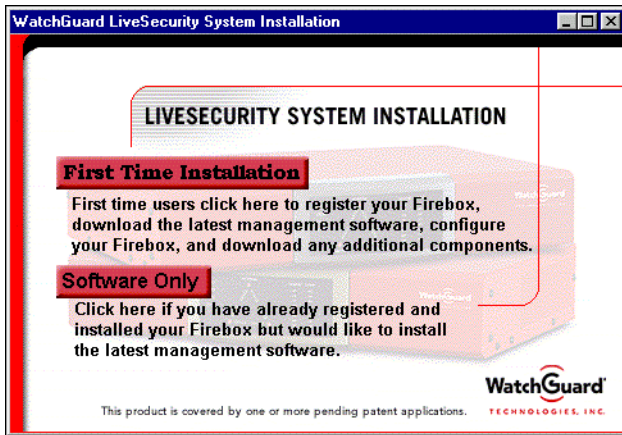
The LiveSecurity System integrated installation wizard installs the LiveSecurity Service, registers your LiveSecurity license key, and downloads and installs the Management Station software.



- Management Station with 20 MB space on the local hard drive
- [Optional] Connection to Internet

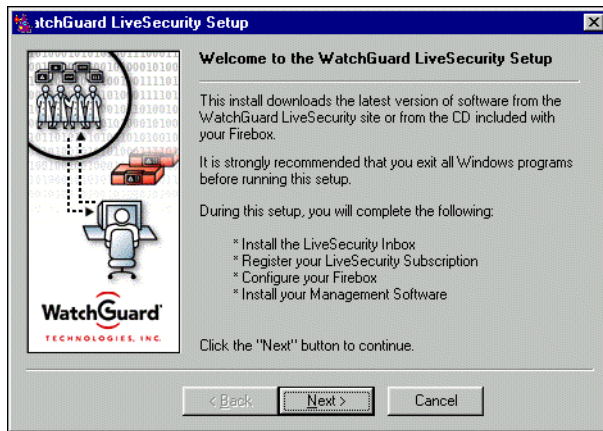
1. Exit all applications on the computer you selected for the LiveSecurity System. Insert the WatchGuard LiveSecurity disk into the CD-ROM drive.

The LiveSecurity installation wizard should start automatically. If it does not, use Windows Explorer® to find `install.exe` in the root directory of the WatchGuard LiveSecurity System CD-ROM. Double-click `install.exe` to start the installation process.

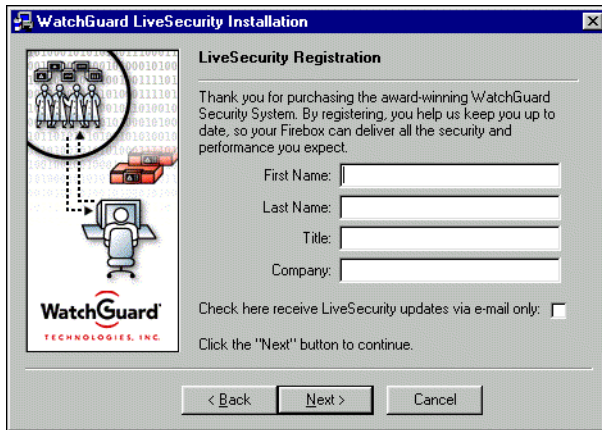


2. Click First Time Install.

The installation utility automatically verifies that you have a working connection to the Internet. In the absence of a working connection, you can install the software but you will not be able to register for LiveSecurity nor will you begin receiving vital information regarding your network security from the LiveSecurity Service.

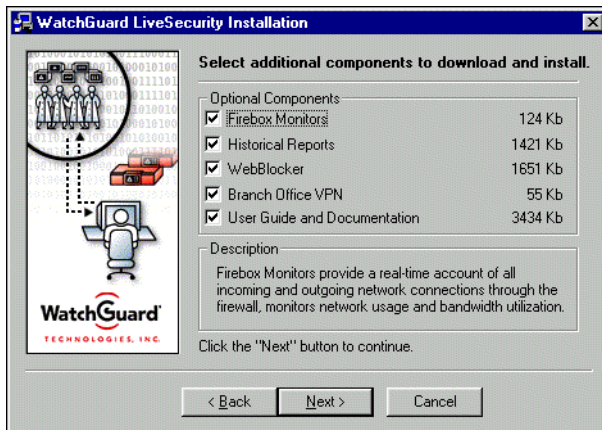


3. Use the Next and Back buttons to move through the installation wizard. Read and accept the license agreement.
4. Select the WatchGuard installation directory. Click Next.
The default installation directory is C:\Program Files\WatchGuard.
5. Select the WatchGuard Start menu directory. Click Next.
The default Start menu location is Start ⇒Program Files ⇒WatchGuard.
6. Enter your LiveSecurity License Key. Click Next.
The License Key number is located on the WatchGuard LiveSecurity Agreement License Key Certificate. The installation wizard queries the WatchGuard LiveSecurity Archive and verifies the validity of your license key. If there is an error, you will be prompted to reenter the key.
7. Complete the LiveSecurity Registration information screens.
Registration information is sent to the WatchGuard LiveSecurity Archive and your record automatically updated. The profile information helps WatchGuard to target information and updates to your needs. The following tips may assist you with completing the forms.



- The Firebox serial number is displayed in two locations:
 - A small silver sticker on the outside of the shipping box
 - A sticker on the back of the Firebox just below the UPC bar code
 - Your login and password will be e-mailed to the address provided on the registration form. Verify that you entered a valid e-mail address.
8. On the Registration Complete alert, click OK.
 9. Select Install the Latest Software from the Web. Click Next.

If the installation wizard was unable to establish connectivity or you would like to use the older software from the CD-ROM, select Install from the LiveSecurity CD-ROM.



10. Select the WatchGuard components to install. Click Next.

WatchGuard recommends that you install the entire product list. For a brief description of any WatchGuard product, position your mouse over the name. When you click Next, the installation wizard downloads the software from the LiveSecurity Archive and then installs it on your hard drive. This can take several minutes during which a progress indicator marks time.

11. Click Install the LiveSecurity Inbox.

The BackWeb installation wizard opens. BackWeb is the software client used for the LiveSecurity Inbox. As the wizard copies the LiveSecurity Inbox to your computer, it displays a progress indicator. When complete, the wizard displays the Setup Complete dialog box.

12. Enable or disable these checkboxes as appropriate:

I would like to launch BackWeb on startup.

When enabled, the LiveSecurity Inbox BackWeb client starts automatically whenever you reboot your computer. WatchGuard recommends enabling this checkbox (i.e. do check) so that the LiveSecurity client will always monitor for broadcasts.

I would like to launch BackWeb now.

When enabled, the LiveSecurity Inbox BackWeb client starts. WatchGuard recommends leaving this checkbox enabled (i.e. checked). However, you may need to minimize the LiveSecurity Inbox to continue with the LiveSecurity installation.

13. Click Finish.

With some installations, clicking Yes fails to restart the computer. If this occurs, click No. The BackWeb installation wizard closes. Restart your computer manually.

14. On the LiveSecurity Installation wizard, click Finish.

The computer should restart automatically. If it does not, restart your computer manually.

Before Proceeding with the QuickSetup Wizard

Before you proceeding to the QuickSetup Wizard, we strongly recommend reading the following three sections on:

- Locating a Firebox within a Network
- Connecting a Firebox
- Completing the Network Configuration Wizard

Locating a Firebox Within a Network

The most common location for a Firebox is directly behind the Internet router as pictured below:

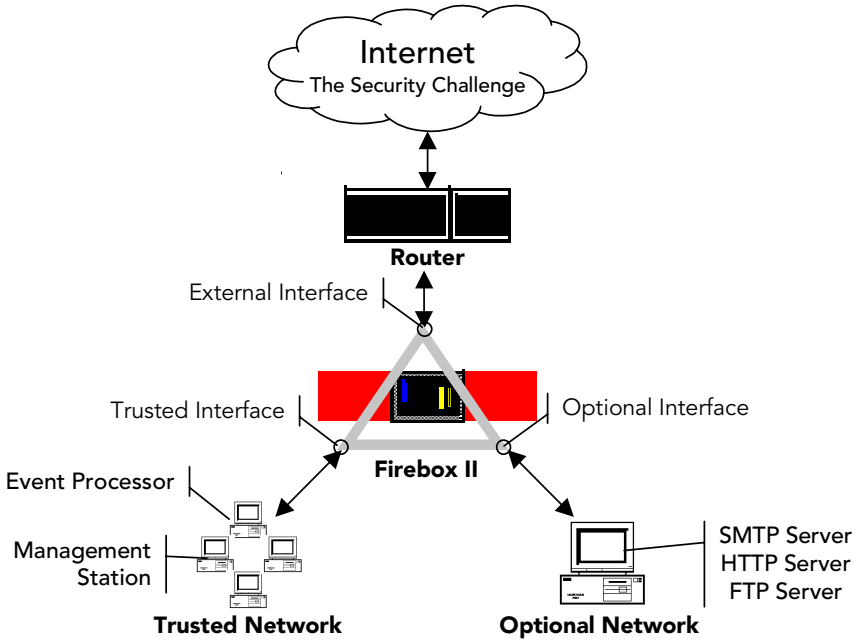
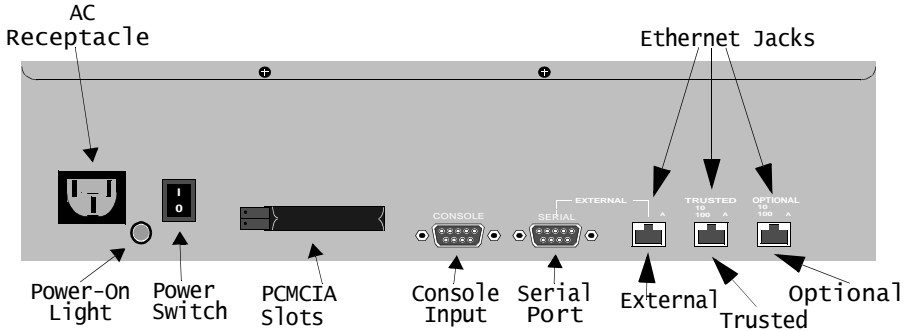


FIGURE 1. Location of Firebox in Network

Connecting a Firebox



There are two methods to connect to and initialize a new Firebox: over a network using TCP/IP or via a serial cable.

Connecting a Firebox for Hands-Free Installation (Recommended)

1. Place the Firebox on a desktop or in a rack in a location convenient to your external router.
2. Use the green cable to connect the Firebox Trusted interface to the same network as your Management Station.
3. Install the power cord from the AC Receptacle on the Firebox to a power source.
4. Flush the ARP cache of the external router.
The most common method to flush a router cache is to cycle the power.
5. When prompted to do so during the QuickSetup Wizard, select Use TCP/IP to Configure as the confirmation access method.

Connecting a Firebox for Serial Cable Initialization

1. Place the Firebox in a location convenient to the Management Station.
2. Use the blue serial cable to connect the Firebox CONSOLE port with the Management Station COM port. Use the red cross-over cable to connect the Trusted interface to the Management Station Ethernet port.
3. Install the power cord from the Firebox AC Receptacle to a power source.
4. When prompted to do so during the QuickSetup Wizard, select Use Serial Cable to Assign IP Address as the configuration access method.

Completing the Network Configuration Worksheet

We encourage you to complete the following network configuration worksheet before installing the WatchGuard LiveSecurity System for the first time. By completing the worksheet, you will be prepared to answer prompts for IP addresses. The resulting basic configuration file will more closely match your true network environment.



NOTE

A standard letter size version of the Network Configuration Worksheet is available in PDF format on the installation CD-ROM in the Documentation folder.

Network Configuration Worksheet

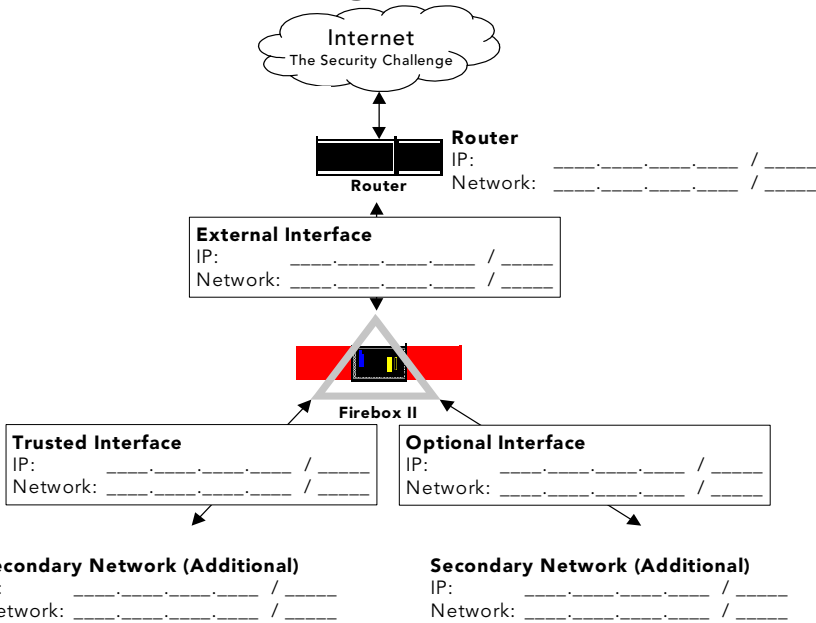


Table 2. Network Configuration Worksheet QuickSetup Wizard Data

Label	IP Addresses
Event Processor	_____
Default Gateway	_____
Firebox Interface (Drop In Only)	_____ / _____
External Interface (Routed Only)	_____ / _____
Trusted Interface (Routed Only)	_____ / _____
Optional Interface (Routed Only)	_____ / _____
Secondary Network	_____ / _____
SMTP Service	_____
HTTP Service (Routed Only)	_____
FTP Service (Routed Only)	_____

Running the QuickSetup Wizard

The final step of the WatchGuard LiveSecurity System installation is to run the QuickSetup Wizard. The QuickSetup Wizard creates a basic configuration file and saves it to the primary area of the Firebox flash disk. The Firebox loads the primary configuration file when it boots.

The QuickSetup Wizard also writes a basic configuration file called `wizard.cfg` to the hard drive of the Management Station. You must then expand the Firebox's basic configuration using the Policy Manager.

By default, the QuickSetup Wizard starts automatically after you complete installing the LiveSecurity System software. To manually start the QuickSetup Wizard from the Windows desktop, select Start ⇒ Programs ⇒ WatchGuard ⇒ QuickSetup Wizard.



The first step of the QuickSetup Wizard prompts you to select a configuration option:

Configure in Drop-In Mode (Recommended)

A drop-in network configuration is useful for situations where you can distribute your network's logical address space across the Firebox's interfaces. In a drop-in configuration, you place the Firebox physically between the router and the LAN, without re-configuring any of the machines on the Trusted interface.

Characteristics of a drop-in configuration:

- A single network not subdivided into smaller networks
- The Firebox performs proxy ARP
- All Trusted computers must have their ARP caches flushed
- All three Firebox interfaces are assigned IP addresses on the same network This is true whether or not you use the Optional interface.
- The majority of a LAN resides on the Trusted interface
- List the IP address of secondary networks in the configuration file

For instructions on configuring your Firebox for drop-in mode, see “Configuring the Firebox in Drop-In Mode” on page 17.

Configure in Routed Mode

A routed network configuration is for situations where the Firebox is put in place with separate logical networks on its interfaces. It assigns separate network addresses to at least two of the three Firebox interfaces.

If you have two separate network addresses and you want to use the routed configuration, use only the External and Trusted interfaces (that is, don't use the Optional interface) because each interface must be on a separate network in routed configuration mode.

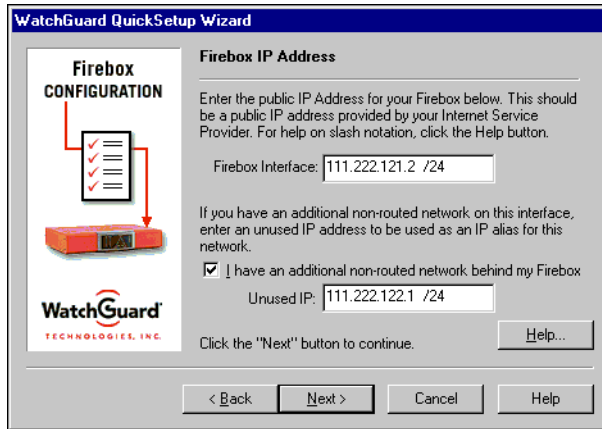
If you have three or more network addresses, use the routed network configuration and map a network to each interface. Add additional networks as secondary networks to one of the interfaces. You can relate different networks to different interfaces. Those networks then come under the protection and access rules set up for that interface. The Firebox forwards packets to the various interfaces depending on how you define and configure services in the Policy Manager.

For instructions on configuring your Firebox for routed mode, see “Configuring the Firebox in Routed Mode” on page 20.

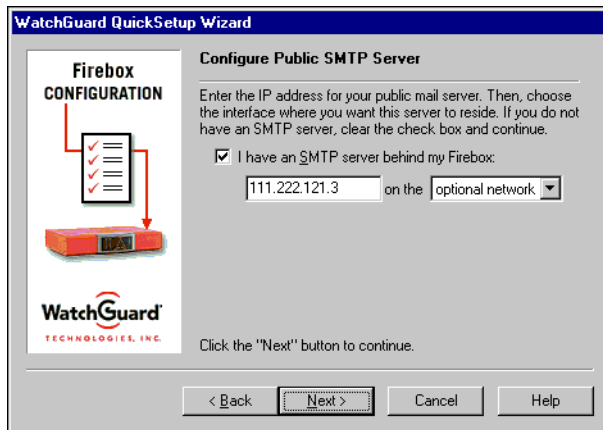
Configuring the Firebox in Drop-In Mode

1. Select Configure in Drop-In Mode. Click Next.
2. Enter the IP address for the Firebox interfaces.

In a drop-in configuration, all three interfaces share the same IP address.

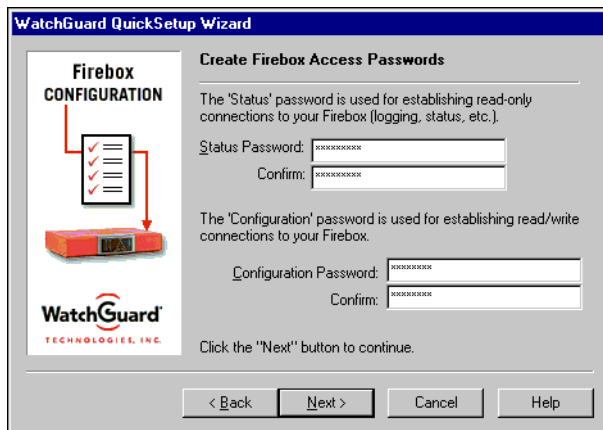


3. If there is a secondary network on the Trusted interface, enable the “I have an additional non-routed network behind my Firebox” checkbox. Enter an unused IP on the secondary network in slash notation. Click Next.
4. Enter the default gateway. Click Next.
5. If you would like to configure an SMTP server, enable the “I have an SMTP server behind my Firebox” checkbox. Enter the SMTP server IP address. Use the drop-list to select whether the server is on the trusted or optional network.



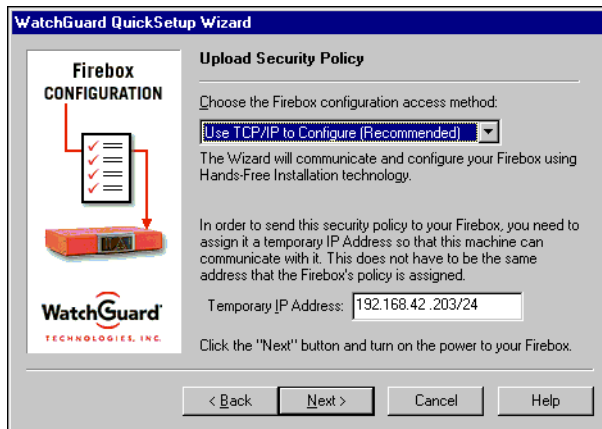
6. Click Next. Enter the Firebox status (read-only) and configuration (read-write) passwords.

You must select two different values for the two password types.



7. Click Next. Select a Configuration Access Method.

If the Firebox is connected to the same network as the Management Station, select Use TCP/IP to Configure for Hands-Free Installation. If the Firebox is connected directly to the Management Station with a blue serial cable, select Use Serial Cable to Assign IP Address for Serial Cable Initialization. When using a serial cable, you must also supply the Management Station serial port number.



8. Click Next.
9. Review the settings. The information is saved to a file named `wizard_setup.txt` in the WatchGuard installation directory. Click OK.
The QuickSetup Wizard creates a basic configuration file and saves it to the local hard drive as `wizard.cfg`. It then attempts to contact the Firebox.
10. Enter the factory installed configuration pass phrase: `wg`. Click OK.
11. Turn the Firebox off and then on again.
The QuickSetup Wizard attempts to connect to the Firebox. If there are multiple Fireboxes with the read-write pass phrase 'wg' on the same network, the Firebox selector dialog box appears. Use the Blink Lights button to select the address of the Firebox you are currently configuring.
12. When a connection is made, the wizard uploads a basic configuration file to the primary area of the Firebox flash disk and initializes the Firebox with the IP addresses you provided. When complete, the Firebox Sys A and Armed indicators light.
13. Go to "After You Install" on page 23.

Configuring the Firebox in Routed Mode

1. Select Configure in Routed Mode. Click Next.
2. Enter the IP address for the Firebox interfaces.

In a routed configuration, the three Firebox interfaces use different addresses.

The screenshot shows the 'WatchGuard QuickSetup Wizard' window. On the left, there is a 'Firebox CONFIGURATION' section with a diagram of a Firebox device and a list of configuration steps, some with checkmarks. Below the diagram is the WatchGuard logo. The main area is titled 'Firebox Interfaces' and contains the following text: 'Enter the Address for each Firebox interface below. You may add one additional network behind the trusted interface if necessary. For help on slash notation, click the Help button.' There are three input fields for 'External Interface:', 'Trusted Interface:', and 'Optional Interface:', each containing '... /'. Below these is a checked checkbox labeled 'I have an additional non-routed network behind my Firebox' with an 'Unused IP:' field containing '... /'. A 'Help...' button is to the right. At the bottom are '< Back', 'Next >', 'Cancel', and 'Help' buttons.

3. If there is a secondary network on the Trusted interface, enable the “I have an additional non-routed network behind my Firebox” checkbox. Enter an unused IP on the secondary network in slash notation. Click Next.
4. Enter the default gateway. Click Next.

The screenshot shows the 'WatchGuard QuickSetup Wizard' window. On the left, there is a 'Firebox CONFIGURATION' section with a diagram of a Firebox device and a list of configuration steps, some with checkmarks. Below the diagram is the WatchGuard logo. The main area is titled 'Configure Public Servers' and contains the following text: 'Enter the IP address(es) for your public servers. If you do not have any public servers, leave the check boxes empty.' There are three checked checkboxes: 'I have an SMTP server behind my Firebox:', 'I have an HTTP server on the optional interface:', and 'I have an FTP server on the optional interface:'. Each checkbox has an associated input field containing '...'. A 'Help...' button is to the right. At the bottom are '< Back', 'Next >', 'Cancel', and 'Help' buttons.

5. If you would like to configure public servers, enable the appropriate checkbox(es). Enter the IP address of each public server. Click Next.

- Enter the Firebox status (read-only) and configuration (read-write) passwords.

You must select two different values.

- Click Next. Select a Configuration Access Method.

If the Firebox is connected to the same network as the Management Station, select Use TCP/IP to Configure for Hands-Free Installation. If the Firebox is connected directly to the Management Station with a blue serial cable, select Use Serial Cable to Assign IP Address for Serial Cable Initialization. When using a serial cable, you must also supply the Management Station serial port number.

- Click Next.
- Review the settings. The information is also saved to a file named wizard_setup.txt in the WatchGuard installation directory. Click OK.

The QuickSetup Wizard creates a basic configuration file and saves it to the local hard drive as wizard.cfg. It then attempts to contact the Firebox.

10. Enter the factory installed configuration pass phrase: wg. Click OK.

11. Turn the Firebox off and then on again.

The QuickSetup Wizard attempts to connect to the Firebox. If there are multiple Fireboxes with the read-write pass phrase 'wg' on the same network, the Firebox selector dialog box appears. Use the Blink Lights button to select the address of the Firebox you are currently configuring.

12. When a connection is made, the wizard uploads a basic configuration file to the primary area of the Firebox flash disk and initializes the Firebox with the IP addresses you provided. When complete, the Firebox SysA and Armed indicators light.

After You Install

Your Firebox can now communicate with the Management Station over your network.

- **If you have not done so already, install the Firebox on your network.**
The most common location is physically between the Internet router and connections to your trusted and optional networks. See “Locating a Firebox Within a Network” on page 11.
- **Connect your Ethernet lines to the Firebox Trusted, External, and Optional interfaces as appropriate.**
Specific connections vary according to the simple or multiple network configuration created. You are not required to connect the Optional interface if it is not part of your network configuration.
- **Reboot the Management Station.**
If you have designated the Management Station as the primary event processor, the LiveSecurity Event Processor starts.
- **Open the *User Guide* for additional configuration instructions.**
- **Using Adobe Acrobat Reader® you can print all or part of the *Reference Guide* and *Internet Security Handbook* for additional information.**

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-4.1-Install-6