
WatchGuard® LiveSecurity™ System Install Guide

LiveSecurity System 4.5



Disclaimer

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 and Patent Information

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

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

Red Hat® is a registered trademark of Red Hat, Inc. This product is not a product of Red Hat, Inc. and is not endorsed by Red Hat, Inc. This is a product of WatchGuard and we have no relationship with Red Hat, Inc.

Adobe, Acrobat, the Acrobat logo, and PostScript are trademarks of Adobe Systems Incorporated.

© 1999 BackWeb Technologies, Inc. All rights reserved. BackWeb is a registered trademark of BackWeb Technologies, Inc.

CyberNOT, CyberNOT List, CyberYES, and CyberYES List are trademarks of Learning Company Properties Inc.

© Hi/fn, Inc. 1993, including one or more U.S. Patents: 4701745, 5016009, 5126739, and 5146221 and other patents pending.

© 1995-1998 Eric Young (eay@cryptsoft). All rights reserved.

© 1998-1999 The OpenSSL Project. All rights reserved.

Java and all Java-based marks are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

Microsoft®, Internet Explorer®, Windows® 95, Windows® 98, Windows NT® and Windows® 2000 are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Netscape and Netscape Navigator are registered trademarks of Netscape Communications Corporation in the United States and other countries.

RC2 Symmetric Block Cipher, RC4 Symmetric Stream Cipher, RC5 Symmetric Block Cipher, BSAFE, TTPEM, RSA Public Key Cryptosystem, MD, MD2, MD4, and MD5 are either trademarks or registered trademarks of RSA Data Security, Inc. Certain materials herein are Copyright © 1992-1999 RSA Data Security, Inc. All rights reserved.

RealNetworks, RealAudio, and RealVideo are either a registered trademark or trademark of RealNetworks, Inc. in the United States and/or other countries.

VPCOM™ Copyright © 1997-1999 Ashley Laurent, Inc. All rights reserved.

All other trademarks and tradenames are the property of their respective owners.

Printed in the United States of America.

DocVer: S-45-Install-2

WatchGuard Technologies, Inc.

LiveSecurity System Software (LSS)

End-User License Agreement

IMPORTANT - READ CAREFULLY BEFORE ACCESSING WATCHGUARD SOFTWARE:

This LSS End-User License Agreement (the "AGREEMENT") is a legal agreement between you (either an individual or a single entity) and WatchGuard Technologies, Inc. ("WATCHGUARD") for the WATCHGUARD LSS Software you have purchased, which includes computer software, any separately installed components, and any updates or modifications thereto, and which may include associated media, printed materials, and online or electronic documentation ("SOFTWARE PRODUCT"). WATCHGUARD is willing to license the SOFTWARE PRODUCT to you only on the condition that you accept all of the terms contained in this AGREEMENT. Please read this AGREEMENT carefully. By installing or using the SOFTWARE PRODUCT you agree to be bound by the terms of this AGREEMENT. If you do not agree to the terms of this AGREEMENT, WATCHGUARD will not license the SOFTWARE PRODUCT to you, and you will not have any rights in the SOFTWARE PRODUCT. In that case, promptly return the SOFTWARE PRODUCT, along with proof of payment, to the authorized dealer from whom you obtained the SOFTWARE PRODUCT for a full refund of the price you paid.

1. **Ownership and License.** The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. This is a license agreement and NOT an agreement for sale. All title and copyrights in and to the SOFTWARE PRODUCT (including, but not limited to, any images, photographs, animations, video, audio, music, text, and applets incorporated into the SOFTWARE PRODUCT) and any copies of the SOFTWARE PRODUCT are owned by WATCHGUARD or its suppliers. Your rights to use the SOFTWARE PRODUCT are as specified in this AGREEMENT, and WATCHGUARD retains all rights not expressly granted to you in this AGREEMENT. Nothing in this AGREEMENT constitutes a waiver of the rights of WATCHGUARD under U.S. copyright law or any other law or treaty.

2. **Permitted Uses.** You are granted the following rights to the SOFTWARE PRODUCT:

(A) You may install and use the SOFTWARE PRODUCT on any single computer at any single location where you conduct your business operations. If you wish to use the SOFTWARE PRODUCT on a different computer, you must erase the SOFTWARE PRODUCT from the first computer on which you installed it before you install it onto a second.

(B) To use the SOFTWARE PRODUCT on more than one computer at once, you must license an additional copy of the SOFTWARE PRODUCT for each additional computer on which you want to use it.

(C) You may make a single copy of the SOFTWARE PRODUCT for backup or archival purposes only.

3. **Prohibited Uses.** You may not, without express written permission from WATCHGUARD:

(A) Use, copy, modify, merge or transfer copies of the SOFTWARE except as provided in this AGREEMENT;

(B) Use any backup or archival copy of the SOFTWARE PRODUCT (or allow someone else to use such a copy) for any purpose other than to replace the original copy in the event it is destroyed or becomes defective;

(C) Sublicense, lend, lease or rent the SOFTWARE PRODUCT;

(D) Transfer this license to another party unless:

(i) the transfer is permanent;

(ii) the third party recipient agrees to the terms of this AGREEMENT, and

(iii) you do not retain any copies of the SOFTWARE PRODUCT; or

(E) Reverse engineer, disassemble or decompile the SOFTWARE PRODUCT.

4. Limited Warranty. WATCHGUARD makes the following limited warranties for a period of ninety (90) days from the date you obtained the SOFTWARE PRODUCT from WATCHGUARD or an authorized dealer:

(A) Media. The disks and documentation will be free from defects in materials and workmanship under normal use. If the disks or documentation fail to conform to this warranty, you may, as your sole and exclusive remedy, obtain a replacement free of charge if you return the defective disk or documentation to us with a dated proof of purchase.

(B) SOFTWARE PRODUCT. The SOFTWARE PRODUCT will materially conform to the documentation that accompanies it. If the SOFTWARE PRODUCT fails to operate in accordance with this warranty, you may, as your sole and exclusive remedy, return the SOFTWARE PRODUCT and the documentation to the authorized dealer from whom you obtained it, along with a dated proof of purchase, specifying the problems, and such authorized dealer will provide you with a new version of the SOFTWARE PRODUCT or a full refund, at their election.

Disclaimer and Release. THE WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD, AND YOUR REMEDIES, SET FORTH IN PARAGRAPHS 4, 4(A) AND 4(B) ABOVE ARE EXCLUSIVE AND IN SUBSTITUTION FOR, AND YOU HEREBY WAIVE, DISCLAIM AND RELEASE ANY AND ALL OTHER WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD AND ALL OTHER RIGHTS, CLAIMS AND REMEDIES YOU MAY HAVE AGAINST WATCHGUARD, EXPRESS OR IMPLIED, ARISING BY LAW OR OTHERWISE, WITH RESPECT TO ANY NONCONFORMANCE OR DEFECT IN THE SOFTWARE PRODUCT (INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ANY IMPLIED WARRANTY ARISING FROM COURSE OF PERFORMANCE, COURSE OF DEALING, OR USAGE OF TRADE, ANY WARRANTY OF NONINFRINGEMENT, ANY WARRANTY THAT THIS SOFTWARE PRODUCT WILL MEET YOUR REQUIREMENTS, ANY WARRANTY OF UNINTERRUPTED OR ERROR-FREE OPERATION, ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY IN TORT, WHETHER OR NOT ARISING FROM THE NEGLIGENCE (WHETHER ACTIVE, PASSIVE OR IMPUTED) OR FAULT OF WATCHGUARD AND ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY FOR LOSS OR DAMAGE TO, OR CAUSED BY OR CONTRIBUTED TO BY, THE SOFTWARE PRODUCT).

Limitation of Liability. WATCHGUARD'S LIABILITY (WHETHER IN CONTRACT, TORT, OR OTHERWISE; AND NOTWITHSTANDING ANY FAULT, NEGLIGENCE, STRICT LIABILITY OR PRODUCT LIABILITY) WITH REGARD TO THE SOFTWARE PRODUCT WILL IN NO EVENT EXCEED THE PURCHASE PRICE PAID BY YOU FOR SUCH PRODUCT. IN NO EVENT WILL WATCHGUARD BE LIABLE TO YOU OR ANY THIRD PARTY, WHETHER ARISING IN CONTRACT (INCLUDING WARRANTY), TORT (INCLUDING ACTIVE, PASSIVE OR IMPUTED NEGLIGENCE AND STRICT LIABILITY AND FAULT), FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF OR IN CONNECTION WITH THIS WARRANTY OR THE USE OF OR INABILITY TO USE THE SOFTWARE PRODUCT, EVEN IF WATCHGUARD HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

5. United States Government Restricted Rights. The enclosed SOFTWARE PRODUCT and documentation are provided with Restricted Rights. Use, duplication or disclosure by the U.S. Government or any agency or instrumentality thereof is subject to restrictions as set forth in subdivision (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013, or in subdivision (c)(1) and (2) of the Commercial Computer Software -- Restricted Rights Clause at 48 C.F.R. 52.227-19, as applicable. Manufacturer is WatchGuard Technologies, Incorporated, 505 Fifth Avenue South, Suite 500, Seattle, WA 98104.

6. Export Controls. You agree not to directly or indirectly transfer the SOFTWARE PRODUCT or documentation to any country to which such transfer would be prohibited by the U.S. Export Administration Act and the regulations issued thereunder.

7. Termination. This license and your right to use the SOFTWARE PRODUCT will automatically terminate in the event you (i) fail to comply with any provisions of this AGREEMENT; (ii) destroy

all copies of the SOFTWARE PRODUCT in your possession, or; (iii) voluntarily return the SOFTWARE PRODUCT to WATCHGUARD. Upon termination you will destroy all copies of the SOFTWARE PRODUCT and documentation remaining in your control or possession.

8. Miscellaneous Provisions. This AGREEMENT will be governed by and construed in accordance with the substantive laws of Washington excluding the 1980 United National Convention on Contracts for the International Sale of Goods, as amended. This is the entire AGREEMENT between us relating to the contents of this package, and supersedes any prior purchase order, communications, advertising or representations concerning the contents of this package AND BY USING THE SOFTWARE PRODUCT YOU AGREE TO THESE TERMS. No change or modification of this AGREEMENT will be valid unless it is in writing, and is signed by WATCHGUARD.

9. Canadian Transactions: If you obtained this SOFTWARE PRODUCT in Canada, you agree to the following:

The parties hereto have expressly required that the present AGREEMENT and its Exhibits be drawn up in the English language. / Les parties aux presentes ont expressement exige que la presente conventions et ses Annexes soient redigees en la langue anglaise.

Declaration of Conformity

WatchGuard Technologies, Inc.
505 Fifth Avenue South
Suite 500
Seattle WA 98104-3892

Declares the CE-marked product:

Product Models:	Firebox II, Firebox II <i>Plus</i> , Firebox II FastVPN	
Complies with:	73/23/EEC Low Voltage Directive 89/336/EEC Electromagnetic Compatibility Directive	
Compliance Standards:	EN60950:1992	Electrical Safety A1:1993, A2:1993, A3:1995, A4:1997, A11:1997
	EN55022, Class A	RF Emissions Information Technology
	EN50082-1	EMC Immunity Standard

FCC Certification

This device has been tested and found to comply with limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

CE Notice

The official CE symbol indicates compliance of this WatchGuard Technologies, Inc. product to the EMC directive of the European Community. The CE symbol found here or elsewhere indicates that this WatchGuard product meets or exceeds the following standards:

EN60950:1992	Electrical Safety A1:1993, A2:1993, A3:1995, A4:1997, A11:1997
EN55022,Class A	RF Emissions Information Technology
EN50082-1	EMC Immunity Standard



CSA Statement

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

WatchGuard LiveSecurity System Install Guide

The WatchGuard LiveSecurity System is an interdependent system of distributed software, downloadable software, the Firebox, Event Processor and the computer used to administer the Firebox (the Management Station). This document walks you through the installation, step-by-step to ensure a smooth installation. This document should also provide you with basic understanding of what is downloaded, expanded, installed, and configured.

Documentation

All WatchGuard LiveSecurity System documentation is installed along with the LiveSecurity software. 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.

Notational Conventions

WatchGuard manuals use the following notational conventions:

-
-
- When instructed to select a menu command from a cascading menu, the command names are separated by an arrow (⇒). For example, if the text says to: Select **File** ⇒ **Open**, this means to click the **File** menu and then click the **Open** command.
 - Web-site addresses appear in a sans-serif font. For example:
`http://www.watchguard.com`
 - Code and directory entries appear in a sans-serif font. For example:
`[WatchGuard installation directory]\RUVPN\Exp`

Before You Install

Terms You Should Know

The following terms are commonly used by WatchGuard when referring to our product and how it is implemented.

- **Management Station** — The computer on which to install and run the WatchGuard LiveSecurity Control Center software.
- **Event Processor** — The computer that receives and stores log messages and issues notifications. The Management Station can also serve as the event processor.
- **WatchGuard LiveSecurity Service** — The network that transmits security alerts, editorials, threat responses, and software updates directly to your desktop.
- **LiveSecurity Inbox** — The client software for the LiveSecurity Service.
- **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 configuration in which the Firebox is physically located between the router and the LAN without any of the

computers on the Trusted interface being reconfigured. This protects a single network that is not subdivided into smaller networks.

- **Routed Configuration** —A configuration with separate network addresses assigned to at least two of the three Firebox interfaces. This type of configuration is intended for situations in which the Firebox is put in place with separate logical networks on its interfaces.
- **Secondary Network** — A network on the same physical wire as a Firebox interface that has an address belonging to an entirely different network.

Selecting Computers

One of the first tasks before installing the WatchGuard LiveSecurity Service is to determine the computers to use for different functions in the security system:

- **Choose the computer to use for the Management Station.**
The Management Station operating system platform must be Windows 95, Windows 98, Windows NT (Service Pack 4, 5, or 6a), or Windows 2000.
- **Choose the computer to use for the LiveSecurity Service. Verify that it has access to the Internet using Microsoft Internet Explorer® 4.0 (or later) or Netscape Communicator® 4.5 (or later).**
WatchGuard recommends using the Management Station computer as the computer for the LiveSecurity Service. However, if the configuration requires it, designate an alternate computer by running LSClient.exe, which is located on the CD. (Also download LSClient.exe from the LiveSecurity Service Web site.)
- **Choose the computer to use for the primary event processor.**
If not using the Management Station computer for the Event Processor, download a new LSEP package from the LiveSecurity Service Web site.

Software Requirements

WatchGuard LiveSecurity System version 4.5 can run on Microsoft Windows 95, Windows 98, Windows NT 4.0, or Windows 2000 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 Service Pack 4, 5, or 6a

Windows 2000 Requirements

- Microsoft Windows 2000 SR1

Web Browser Requirements

Microsoft Internet Explorer® 4.0 or higher is required to run the installation from the CD. The following HTML-based browsers are recommended to view WatchGuard Online Help:

- Netscape Communicator® 4.7 or later
- Microsoft Internet Explorer® 5.01 or later



Microsoft Internet Explorer 5.5 is currently not supported.

Hardware Requirements

Hardware minimum requirements are the same as for the operating system on which WatchGuard LiveSecurity System 4.5 runs. The recommended hardware ranges are listed below:

Table 1. WatchGuard LSS 4.5 Hardware Requirements

Hardware Feature	Minimum Requirement
CPU	Pentium II
Memory	Same as for operating system; Recommended: 32 MB for Windows 95 64 MB for Windows 98 64 MB for Windows NT 4.0 64 MB for Windows 2000 Professional 256 MB for Windows 2000 Server

Table 1. WatchGuard LSS 4.5 Hardware Requirements

Hardware Feature	Minimum Requirement
Hard Disk Space	25 MB to install all WatchGuard modules 15 MB minimum for log file 10 MB for LiveSecurity Inbox 50 MB for Inbox content 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 4.5 from Previous Versions

Before upgrading, make sure to perform the following

1. Make a copy of the current Firebox configuration file.
2. Exit and disable the WatchGuard Event Processor.



If you are running Windows NT, disabling the Event Processor does not stop the service. Stop the service first, either from the Event Processor interface or from Control Panel.

3. Uninstall any previous versions of WatchGuard software.

Installing the LiveSecurity System

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



- Management Station with 20 MB space on the local hard drive, 50 MB for Inbox content.
- [Optional] Connection to Internet

1. Exit all applications on the computer 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 Watch-

Guard LiveSecurity System CD-ROM. Double-click `install.exe` to start the installation process.

2. Click **Activate LiveSecurity Service**. The installation program automatically verifies whether or not there is an Internet connection. This is an important step. The LiveSecurity Service updates you whenever there is an alert that is important to you.
3. The LiveSecurity installation wizard begins. Use the **Next** and **Back** buttons to move through the installation wizard.

Before Proceeding with the QuickSetup Wizard

Before proceeding to the QuickSetup read the following three sections:

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

Locating a Firebox Within a Network

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

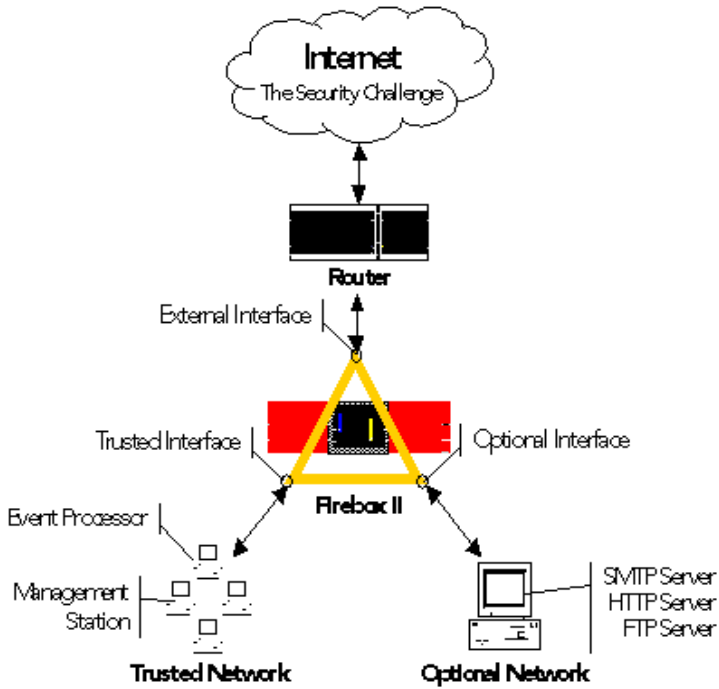
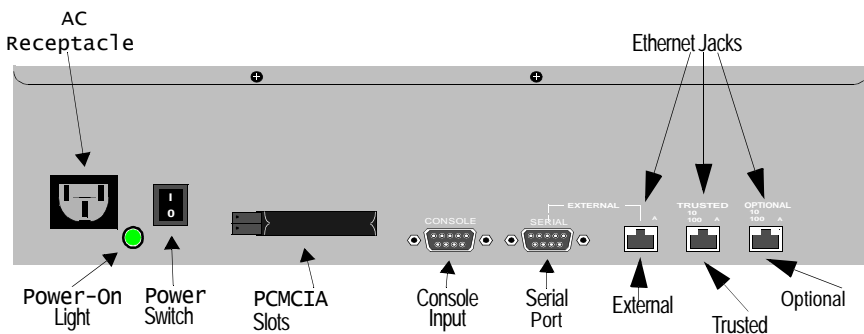


FIGURE 1. Location of Firebox in Network

Connecting a Firebox



You can connect to and initialize a new Firebox in two ways: over a network using TCP/IP or via a serial cable.

Connecting a Firebox for Hands-Free Installation

This process automatically gives the Firebox an IP address.

1. Place the Firebox on a desktop or in a rack in a location convenient to the external router.
2. Use the green (non-crossover) cable (provided with the Firebox) to connect the Firebox Trusted interface to the same network as the Management Station.
3. Install the power cord from the AC Receptacle on the Firebox to a power source.
4. 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

This process requires that you manually create an IP address.

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 network configuration worksheet on the following page 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 the true network environment.



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

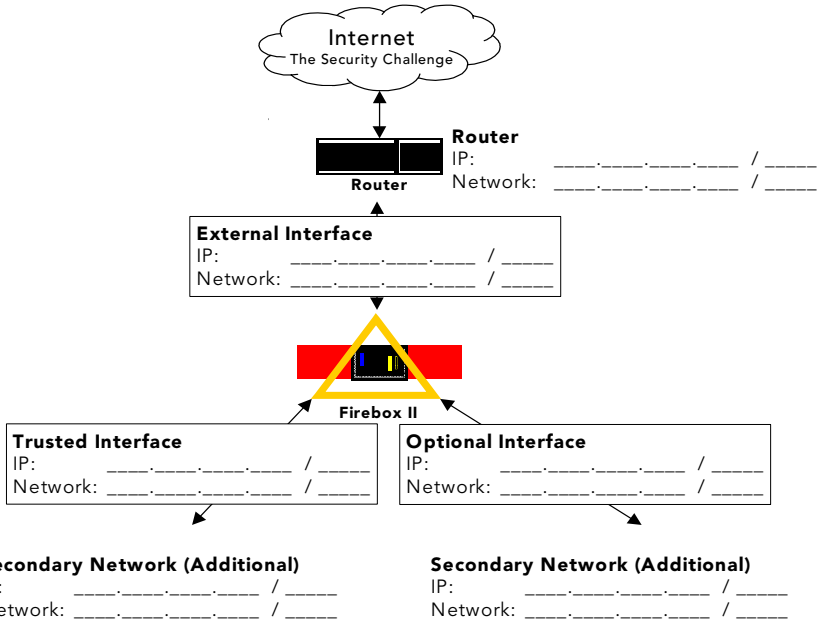


Table 2. Network Configuration Worksheet QuickSetup Wizard Data

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)	_____

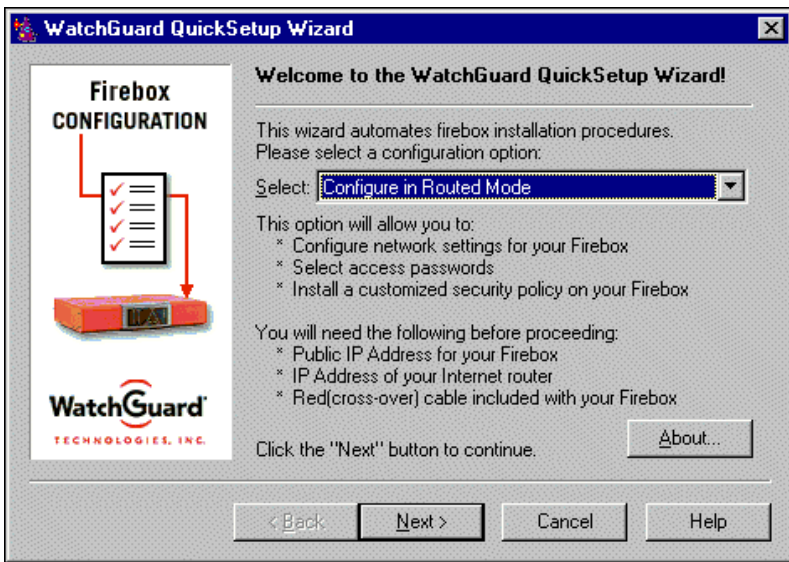
Running the QuickSetup Wizard

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 Management Station hard drive. After completing the QuickSetup Wizard, customize 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: either drop-in mode or routed mode. These configurations are described in the next two sections.



Drop-In Mode

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

Characteristics of a drop-in configuration:

- A single IP network not subdivided into smaller IP networks.
- The Firebox performs proxy ARP.
- All Trusted computers must have their ARP caches flushed or timed out.
- All three Firebox interfaces are assigned the same IP address on all the interfaces.
- 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 13.

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 there are two separate network addresses and you want to use the routed configuration, use only the External and Trusted interfaces (do not use the Optional interface). Each interface must be on a separate network in routed configuration mode.

If there are 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 14.

Configuring the Firebox in Drop-In Mode

Use the following procedure to configure a Firebox for 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. 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) pass phrases.
You must select two different values for the two pass phrase types.
7. Click **Next**. Select a configuration access method.



NOTE

While the Quick Start wizard configures the Firebox from any Ethernet interface, the Firebox only allows configuration access through the Trusted interface once the setup is complete.

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. Click **OK**.
The information is saved to a file named wizard_setup.txt in the WatchGuard installation directory. 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.

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

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.

12. Go to “After You Install” on page 15.

Configuring the Firebox in Routed Mode

Use the following procedure to configure a Firebox for 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.
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. To configure public servers, enable the appropriate checkbox(es). Enter the IP address of each public server. Click **Next**.
6. Enter the Firebox status (read-only) and configuration (read-write) pass phrases. These pass phrases must be at least seven characters long.
You must select two different values.
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. 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.
The information is also saved to a file named wizard_setup.txt in the WatchGuard installation directory.
10. Enter the factory installed configuration pass phrase: wg. Click **OK**.

11. Turn the Firebox off and then on.

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.

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

The Firebox can now communicate with the Management Station over the network. Perform the following post-installation steps:

- **If you have not done so already, install the Firebox on the network. Initially this is done over the Trusted interface. You are now ready to customize your security policies.**

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 6.

- **Connect the 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.**
- **You can use Adobe Acrobat Reader® to print all or part of the *Reference Guide* and *Network Security Handbook* for additional information.**

