

WatchGuard® Firebox® SOHO 6 User Guide

SOHO 6.1



Using this Guide

To use this guide you need to be familiar with your computer's operating system. If you have questions about navigating in your computer's environment, please refer to your system user manual.

The following conventions are used in this guide.

Convention	Indication
Bold type	Menu commands, dialog box options, Web page options, Web page names. For example: "On the System Information page, select Disabled."
NOTE	Important information, a helpful tip or additional instructions.

Certifications and Notices

FCC Certification

This appliance has been tested and found to comply with limits for a Class A digital appliance, pursuant to Part 15 of the FCC Rules.

Operation is subject to the following two conditions:

- This appliance may not cause harmful interference.
- This appliance must accept any interference received, including interference that may cause undesired operation.

CE Notice

The CE symbol on your WatchGuard Technologies equipment indicates that it is in compliance with the Electromagnetic Compatibility (EMC) directive and the Low Voltage Directive (LVD) of the European Union (EU).



Industry Canada

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.

VCCI Notice Class A ITE

この装置は、情報処理装置等電波障害自主規制協議会 (VCCI) の基準に基づくクラス A 情報技術装置です。この装置を家庭用環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Declaration of Conformity

DECLARATION OF CONFORMITY

WatchGuard Technologies, Inc.
505 Fifth Ave. S., Suite 500
Seattle, WA 98104-3892
USA

WatchGuard Technologies Inc. hereby declares that the product(s) listed below conform to the European Union directives and standards identified in this declaration.

Product (s):

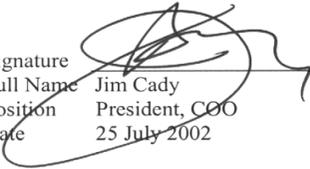
Internet Firewall, Model B0F4S16E6

EU Directive(s):

Low Voltage (73/23/EEC)
Electromagnetic Compatibility (89/336/EEC)

Standard(s):

This product has no safety requirements per the LVD
EN50022 (1998), Class A Emissions for ITE
EN50024 (1998) Immunity for ITE

Signature 
Full Name Jim Cady
Position President, COO
Date 25 July 2002

WATCHGUARD SOHO SOFTWARE END-USER LICENSE AGREEMENT

WATCHGUARD SOHO SOFTWARE END-USER LICENSE AGREEMENT

IMPORTANT - READ CAREFULLY BEFORE ACCESSING WATCHGUARD SOFTWARE

This WatchGuard SOHO Software End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and WatchGuard Technologies, Inc. ("WATCHGUARD") for the WATCHGUARD SOHO software product, which includes computer software (whether installed separately on a computer workstation or on the WatchGuard hardware product) and may include associated media, printed materials, and on-line or electronic documentation, and any updates or modifications thereto, including those received through the WatchGuard LiveSecurity service (or its equivalent) (the "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 EULA. Please read this EULA carefully.

By installing or using the SOFTWARE PRODUCT you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, 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), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT are owned by WATCHGUARD or its licensors. Your rights to use the SOFTWARE PRODUCT are as specified in this EULA, and WATCHGUARD retains all rights not expressly granted to you in this EULA. Nothing in this EULA constitutes a waiver of our rights 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 use the SOFTWARE PRODUCT solely for the purpose of operating the SOHO hardware product in accordance with the SOHO or user documentation.

If you are accessing the SOFTWARE PRODUCT via a Web based installer program,

you are granted the following additional rights to the SOFTWARE PRODUCT:

(A) You may install and use the SOFTWARE PRODUCT on any computer with an associated connection to the SOHO hardware product

in

accordance with the SOHO user documentation;

(B) You may install and use the SOFTWARE PRODUCT on more than one computer

at once without licensing an additional copy of the SOFTWARE PRODUCT for each additional computer on which you want to use it, provided that each computer on which you install the SOFTWARE PRODUCT has an associated connection to the same SOHO hardware product

; and

(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) Reverse engineer, disassemble or decompile the SOFTWARE PRODUCT;
- (B) Use, copy, modify, merge or transfer copies of the SOFTWARE PRODUCT or printed materials except as provided in this EULA;
- (C) 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;
- (D) Sublicense, lend, lease or rent the SOFTWARE PRODUCT; or
- (E) Transfer this license to another party unless
 - (i) the transfer is permanent,
 - (ii) the third party recipient agrees to the terms of this EULA, and
 - (iii) you do not retain any copies of 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; and
- (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 all of 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 they 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 ITS LICENSORS AND ALL OTHER RIGHTS, CLAIMS AND REMEDIES YOU MAY HAVE AGAINST WATCHGUARD AND ITS LICENSORS, 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. THIS WILL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF AN AGREED REMEDY. 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. THIS WILL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF AN AGREED REMEDY.

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 5th Ave. 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 if you fail to comply with any provisions of this EULA, destroy all copies of the SOFTWARE PRODUCT in your possession, or 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 EULA 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 EULA between us relating to the contents of this package, and supersedes any prior purchase order, communications, advertising or representations concerning the SOFTWARE PRODUCT AND BY USING THE SOFTWARE PRODUCT YOU AGREE TO THESE TERMS. IF THE SOFTWARE PRODUCT IS BEING USED BY AN ENTITY, THE INDIVIDUAL INDICATING AGREEMENT TO THESE TERMS REPRESENTS AND WARRANTS THAT (A) SUCH INDIVIDUAL IS DULY AUTHORIZED TO ACCEPT THIS EULA ON BEHALF OF THE ENTITY AND TO BIND THE ENTITY TO THE TERMS OF THIS EULA; (B) THE ENTITY HAS THE FULL POWER, CORPORATE OR OTHERWISE, TO ENTER INTO THIS EULA AND PERFORM ITS OBLIGATIONS UNDER THIS EULA AND; (C) THIS EULA AND THE PERFORMANCE OF THE ENTITY'S OBLIGATIONS UNDER THIS EULA DO NOT VIOLATE ANY THIRD-PARTY AGREEMENT TO WHICH THE ENTITY IS A PARTY.

No change or modification of this EULA will be valid unless it is in writing, and is signed by WATCHGUARD.

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 - 2002 WatchGuard Technologies, Inc. All rights reserved.

AppLock®, AppLock®/Web, Designing peace of mind®, Firebox®, Firebox® 1000, Firebox® 2500, Firebox® 4500, Firebox® II, Firebox® II Plus, Firebox® II FastVPN, Firebox® III, Firebox® SOHO, Firebox® SOHO 6, Firebox® SOHO 6tc, Firebox® SOHO|tc, Firebox® V100, Firebox® V80, Firebox® V60, Firebox® V10, LiveSecurity®, LockSolid®, RapidStream®, RapidCore®, ServerLock®, WatchGuard®, WatchGuard® Technologies, Inc., DVCP™ technology, Enforcer/MUVPN™, FireChip™, HackAdmin™, HostWatch™, Make Security Your Strength™, RapidCare™, SchoolMate™, ServiceWatch™, Smart Security. Simply Done.™, Vcontroller™, VPNforce™ are either registered trademarks or trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries.

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

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, TPEM, 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.

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

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

© 1998-2000 The OpenSSL Project. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)" THIS SOFTWARE IS PROVIDED BY THE OPENSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

© 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

The `mod_ssl` package falls under the Open-Source Software label because it's distributed under a BSD-style license. The detailed license information follows.
Copyright (c) 1998-2001 Ralf S. Engelschall. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the `mod_ssl` project (<http://www.modssl.org/>)."

4. The names "`mod_ssl`" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact rse@engelschall.com.
5. Products derived from this software may not be called "`mod_ssl`" nor may "`mod_ssl`" appear in their names without prior written permission of Ralf S. Engelschall.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the `mod_ssl` project (<http://www.modssl.org/>)."

THIS SOFTWARE IS PROVIDED BY RALF S. ENGELSCHALL ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL RALF S. ENGELSCHALL OR HIS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,

EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The Apache Software License, Version 1.1
Copyright (c) 2000 The Apache Software Foundation. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment:

"This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>)."
Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

4. The names "Apache" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.

5. Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see <<http://www.apache.org/>>.

Portions of this software are based upon public domain software originally written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign.

All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.
Part No 0814-000

Contents

CHAPTER 1 Introduction	1
The Package Contents	2
How Does a Firewall Work?	3
How Does Information Travel on the Internet?	4
<i>IP addresses</i>	4
<i>Protocol</i>	4
<i>Port numbers</i>	5
How Does the SOHO 6 Process Information?	5
<i>Services</i>	5
<i>Network Address Translation</i>	5
The SOHO 6 Hardware Description	6
<i>The SOHO 6 front and rear views</i>	6
CHAPTER 2 Installation	11
Before You Begin	12
<i>Review and record your current TCP/IP settings</i>	12

<i>Disable the HTTP proxy setting of your Web browser</i>	14
<i>Enable your computer for DHCP</i>	16
Physically connect the SOHO 6	18
<i>Cabling the SOHO 6 for one to four appliances</i>	19
<i>Cabling the SOHO 6 for more than four computers</i>	20
CHAPTER 3 SOHO 6 Basics	23
The SOHO 6 Home Page—System Status	23
Default Factory Settings	25
<i>Reset a SOHO 6 to factory default</i>	26
<i>The base model SOHO 6</i>	27
Register your SOHO 6 and Activate the LiveSecurity Service	27
Reboot the SOHO 6	28
CHAPTER 4 Configure the Network Interfaces	31
Configure Your External Network	31
<i>Network addressing</i>	31
<i>Configure the SOHO 6 External Network for dynamic addressing</i>	32
<i>Configure the SOHO 6 External Network for static addressing</i>	33
<i>Configure the SOHO 6 External Network for PPPoE</i>	34
Configure the Trusted Network	36
<i>Configure DHCP Server and DHCP Relay</i>	36
<i>Configure additional computers on the Trusted Network</i>	38
<i>Configure the Trusted Network with static addresses</i>	39
Configure Static Routes	40
View Network Statistics	42

Configure the Dynamic DNS Service	43
Configure OPT Port Upgrades	44
<i>Configure Dual ISP Port</i>	44
<i>Configure VPNforce™ Port</i>	47
CHAPTER 5 Administrative Options	51
The System Security Page	52
<i>System management</i>	52
<i>SOHO Remote Management</i>	54
Set up VPN Manager Access	54
Update Your Firmware	56
Redeem your SOHO 6 Upgrade Options	57
View the Configuration File	60
CHAPTER 6 Configure the Firewall Settings	61
Firewall Settings	61
Configure Incoming and Outgoing Services	62
<i>Pre-configured Services</i>	62
<i>Create a Custom Service</i>	63
Block External Sites	65
Firewall Options	67
<i>Ping requests received on the External Network</i>	68
<i>Denying FTP access to the Trusted Network</i> <i>interface</i>	68
<i>SOCKS implementation for the SOHO 6</i>	68
<i>Logging all allowed outbound traffic</i>	70
<i>Enable override MAC address for the External</i> <i>Network</i>	71
Create an Unrestricted Pass Through	72

CHAPTER 7	Configure Logging	75
	View SOHO 6 Log Messages	76
	Set up Logging to a WatchGuard Security Event Processor Log Host	77
	Set up Logging to a Syslog Host	79
	Set the System Time	80
CHAPTER 8	VPN—Virtual Private Networking	83
	<i>Why Create a Virtual Private Network?</i>	83
	What You Need	84
	<i>Enable the VPN Upgrade</i>	86
	Step-by-step Instructions for Configuring a SOHO 6 VPN Tunnel	86
	<i>Special Considerations</i>	87
	Frequently Asked Questions	87
	Set Up Multiple SOHO-SOHO VPN Tunnels	89
	Configure Split Tunneling	93
	MUVPN Clients	93
	View the VPN Statistics	94
CHAPTER 9	SOHO 6 WebBlocker	95
	How WebBlocker Works	95
	<i>Web site not in the WebBlocker database</i>	96
	<i>Web site in the WebBlocker database</i>	96
	<i>WatchGuard WebBlocker database unavailable</i>	96
	<i>WebBlocker users and groups</i>	97
	<i>Bypass the SOHO 6 WebBlocker</i>	97
	Purchase and Activate SOHO 6 WebBlocker	97
	Configure the SOHO 6 WebBlocker	98

WebBlocker Categories	103
CHAPTER 10 Support Resources	107
Troubleshooting Tips	107
<i>General</i>	107
<i>Configuration</i>	111
<i>VPN Management</i>	114
Contact Technical support	116
Online Documentation and In-Depth FAQs	116
Special Notices	116
Index	117

Introduction

Welcome

Congratulations on purchasing the ideal solution for providing secure access to the Internet—the WatchGuard® Firebox® SOHO 6 or SOHO 6tc security appliance.



This User Guide is for both the SOHO 6 and the SOHO 6tc—the name SOHO 6 refers to both these appliances throughout this guide. The only difference between them is the ability to create and use a Virtual Private Network (VPN). The VPN option is added to the SOHO 6, while the SOHO 6 tc comes with the VPN option pre-installed.

Your new SOHO 6 provides peace of mind when connecting to the Internet using a high-speed cable or DSL modem, a leased line, or ISDN.

The most current installation and user information is available at the WatchGuard Web site:

<http://support.watchguard.com/sohoresources/>

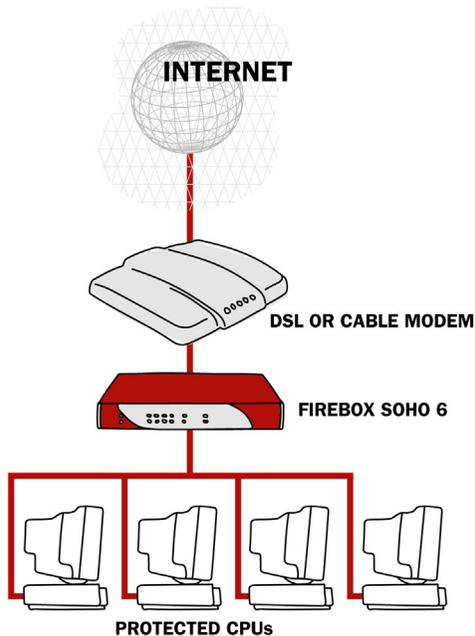
The Package Contents

First things first, check the package contents to make sure you have the following.

- *Firebox SOHO 6 QuickStart Guide*
- User documentation
- AC adapter (12v, 1.0-1.2A)
- Straight-through Ethernet cable
- SOHO 6 security appliance

How Does a Firewall Work?

Fundamentally, a firewall is a way of distinguishing between, as well as protecting, “us” and “them”. On the external side of your SOHO 6 firewall is the entire Internet. The Internet offers many resources such as the Web, email, and video/audio conferencing. It also presents dangers to the privacy and security of your computer. On the trusted side of your SOHO 6 firewall are all the appliances you want to protect from these dangers. As is illustrated in the image below, the SOHO 6 physically separates your trusted network from the Internet.



Using rules or policies outlined in Chapter 3: “Configure Incoming and Outgoing Services” on page 62, the WatchGuard SOHO 6 evaluates all traffic between the external network (the Internet)

and the trusted network (your computer) and blocks any suspicious activity.

How Does Information Travel on the Internet?

All information transported over the Internet is packaged in a special manner to ensure that it travels from one computer to the next. The program responsible for this task is known as TCP/IP. TCP (Transmission Control Protocol) manages the assembly and reassembly of data, for example an email message or program file, into smaller chunks of data called packets. IP (Internet Protocol) takes these packets and wraps them up with a header identifying both where the information is going and how it is handled en route.

IP addresses

An IP address defines the specific computer on the Internet that sends or receives a packet. Every computer on the Internet has a unique address, including your SOHO 6. When defining a service behind a firewall, you need to include the trusted, network address for the computer hosting the application.

On the Internet, IP addresses are identified using a string of numbers that have been translated from a URL (Uniform Resource Locator) name such as, www.watchguard.com.

Protocol

A protocol defines how a packet is bundled and packaged for shipment across a network. The most commonly used protocols are TCP and UDP (User Datagram Protocol). In addition, there are a variety of IP protocols that are less frequently used.

Port numbers

The port numbers are used by computers at both the sending and receiving end to determine the particular program or application for each connection.

How Does the SOHO 6 Process Information?

Services

A service is the combination of protocol(s) and port numbers associated with a specific program or application type. To simplify configuration of your SOHO 6, WatchGuard configured versions of several common services are available for your use.

Network Address Translation

All outgoing connections through a SOHO 6 automatically use a feature called dynamic NAT (Network Address Translation). Without dynamic NAT, your trusted, private addresses are passed along the Internet to their destination.

In addition, the SOHO 6 protects your trusted network by disguising private IP addresses. During an Internet connection, all traffic passed between computers includes IP address information. However, because of the dynamic NAT feature, applications and servers on the Internet only see the public, external IP address of the SOHO 6 itself and are never aware of the addresses in your trusted, network address range.

Imagine that you install a computer behind the SOHO 6 with the IP address 206.253.208.100. If this address were broadcast to the Internet, hackers could easily direct an attack on the computer itself. Instead, the SOHO 6 converts the address automatically to

the external address of the SOHO 6. When a hacker tries to violate the computer, they are stopped at the SOHO 6, never learning the true address of your computer.

The SOHO 6 Hardware Description

The SOHO 6 has significant improvements to the hardware platform from those of previous SOHO models.

Faster Processor

The SOHO 6 has a new network processor running at a speed of 150MHz. It also includes built in Ethernet and encryption technology.

Ethernet ports

The SOHO 6 has six 10/100 Base TX ports labeled OPT, WAN and numbered 0-3.

The SOHO 6 front and rear views

The SOHO 6 has fourteen indicator lights on the front panel of the appliance. The following photograph shows the entire front view.



PWR

When illuminated, this light indicates that the SOHO 6 is currently powered up.

Status

When illuminated, this light indicates that a management connection has been made.

Link

The link indicator illuminates when there is a good physical connection to any of the numbered (0-3) interfaces of the trusted network. The link indicator blinks when traffic is passing through the interface.

100

When a trusted network interface runs at 10Mb, the 100 indicator is *not* illuminated. When the network interface runs at 100 Mb, the 100 indicator is yellow.

WAN

Indicates a good physical connection to the external (WAN) port. The indicator blinks when traffic is passing through the interface.

Mode

Indicates that the SOHO 6 is operational and has connected to the Internet when illuminated.

The SOHO 6 has six Ethernet ports, a reset button, and a power input located on the rear of the appliance. The following photograph shows the entire rear view.



OPT port

This Ethernet port corresponds to the Optional interface. This interface is activated when you purchase the Dual ISP Port upgrade or VPNforce™ Port Upgrade. For more information on the Dual ISP Port and VPNforce Port upgrade, see “Configure OPT Port Upgrades” on page 44.

NOTE

The OPT port is only available if you purchase the Dual ISP Port or VPNforce Port upgrades. You can not use the OPT port as another Ethernet port on the Trusted network.

RESET button

Using the reset button, you can return to the SOHO 6 to the factory defaults. For more information on performing this function, see “Reset a SOHO 6 to factory default” on page 26.

NOTE

The OPT port is only available if you purchase the software upgrades. You can not use the OPT port as another internet port on the Trusted network.

WAN port

This Ethernet port corresponds to the external interface.

4 numbered ports (0-3)

These Ethernet ports correspond to the trusted interface.

Power input

Accepts the 12 volt AC adapter supplied with the SOHO 6.

Installation

This chapter explains how to install the SOHO 6 into your network. You must complete the following steps:

- Review and record your current TCP/IP settings
- Disable the HTTP proxy setting of your Web browser
- Enable your computer for DHCP
- Physically connect the SOHO 6 to your network

For a quick summary of this information, see the *Firebox SOHO 6 QuickStart Guide* included with your SOHO 6.

Before You Begin

Before installing your new SOHO 6, be certain that you have the following items:

- A 10/100BaseT Ethernet I/O network card installed in your computer.
- A cable or DSL modem with a 10/100BaseT port or an ISDN router. This is unnecessary if you connect to the Internet using a LAN connection.
- Two Ethernet network cables with RJ45 connectors. These must *not* be “crossover cables” (often red or orange). One cable is furnished with your SOHO 6. Make certain that both cables are long enough to comfortably connect the modem or router to the SOHO 6 and the SOHO 6 to your computer.
- A functioning Internet connection. If your connection does not work, please contact your ISP (Internet Service Provider).
- Call your ISP to find out which method they use to issue your network addressing—static addresses, DHCP, or PPPoE. You need this information later in the installation process, see “Configure Your External Network” on page 31.
- An installed Web browser—either Netscape Navigator 4.77 (or higher) or Internet Explorer 5.0 (or higher).
- The SOHO 6 serial number.

Review and record your current TCP/IP settings

For your reference, record the computer’s current TCP/IP settings in the chart at the end of this section. Access to this information depends on your computer operating system.

Microsoft Windows 2000 and Windows XP

- 1 Click **Start** ⇒ **Programs** ⇒ **Accessories** ⇒ **Command Prompt**.

- 2 At the default prompt, type `ipconfig/all`, then press **Enter**.
- 3 Enter the TCP/IP settings in the chart provided below.
- 4 Click **Cancel**.

Microsoft Windows NT

- 1 Click **Start** ⇒ **Programs** ⇒ **Command Prompt**.
- 2 At the default prompt, type `ipconfig/all`, then press **Enter**.
- 3 Enter the TCP/IP settings in the chart provided below.
- 4 Click **Cancel**.

Microsoft Windows 95 or 98 or ME

- 1 Click **Start** ⇒ **Run**.
- 2 Type: `winnipcfg`. Click **OK**.
- 3 Select the “Ethernet Adapter.”
- 4 Enter the TCP/IP settings in the chart provided below.
- 5 Click **Cancel**.

Macintosh

- 1 Click the **Apple** menu ⇒ **Control Panels** ⇒ **TCP/IP**.
- 2 Enter the TCP/IP settings in the chart provided below.
- 3 Close the window.

Other operating systems (Unix, Linux)

- 1 Consult your operating system guide to locate the TCP/IP screen.
- 2 Enter the settings in the chart provided below.

3 Exit the TCP/IP configuration screen.

TCP/IP Setting		Value		
IP Address		.	.	.
Subnet Mask		.	.	.
Default Gateway		.	.	.
DHCP Enabled		Yes	No	
DNS Server(s)	Primary	.	.	.
	Secondary	.	.	.

NOTE

If you are connecting more than one computer to the trusted network behind the SOHO 6, determine the TCP/IP settings for each computer.

Disable the HTTP proxy setting of your Web browser

To configure a SOHO 6 after it is installed, you must access the special configuration pages that reside on the SOHO 6. If the HTTP proxy setting in your browser is enabled, you cannot access these pages, making it impossible to complete the configuration process. With the HTTP proxy enabled, the browser automatically points itself to Web pages located on the Internet, and you cannot direct the browser to Web pages located in other places. Disabling the HTTP does not prevent you from accessing your favorite Web sites, but it does allow you to access the configuration pages that reside on the SOHO 6.

To disable the HTTP proxy in three commonly used browsers, see the instructions below. If your browser is not listed, see your browser Help menus to learn how to disable the HTTP proxy settings.

Netscape 4.7

- 1 Open Netscape.
- 2 Click **Edit ⇒ Preferences**.
The Preferences window appears.
- 3 From among the categories listed on the left hand side of the window, click the + symbol before the **Advanced** heading to expand the list.
- 4 Click **Proxies**.
- 5 Verify that the **Direct Connection to the Internet** option is enabled.
- 6 Click **OK** to save the settings.

Netscape 6.x

- 1 Open Netscape.
- 2 Click **Edit ⇒ Preferences**.
The Preferences window appears.
- 3 From among the categories listed on the left side of the window, click the arrow symbol before the **Advanced** heading to expand the list.
- 4 Click **Proxies**.
- 5 Verify that the **Direct Connection to the Internet** option is active.
- 6 Click **OK** to save the settings.

Internet Explorer 5.0, 5.5, and 6.0

- 1 Open Internet Explorer.
- 2 Click **Tools** ⇒ **Internet Options**.
The Internet Options window appears.
- 3 Click the **Advanced** tab.
- 4 Scroll down the page to **HTTP 1.1 Settings**.
- 5 Disable all checkboxes.
- 6 Click **OK** to save the settings.

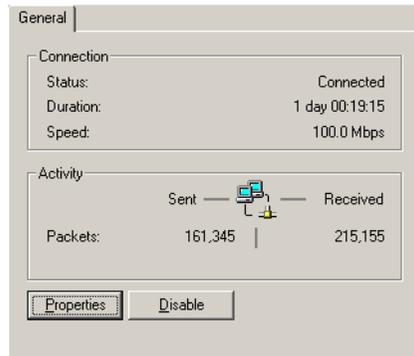
Enable your computer for DHCP

In order to access the special configuration pages on the SOHO 6 after you have physically connected it, your computer must be configured to receive its network IP address by DHCP. For more information regarding network addressing as well as DHCP, see “Network addressing” on page 31.

NOTE

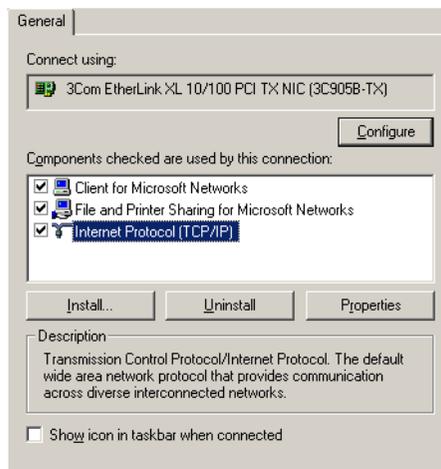
The configuration instructions in this section are for the Windows 2000[®] operating system.

- 1 Click **Start** ⇒ **Settings** ⇒ **Control Panel**.
The Control Panel window appears.
- 2 Double-click the **Network & Dial-up Connections** icon.
- 3 Double-click on the connection you use to access the Internet.
The network connection dialog box appears.



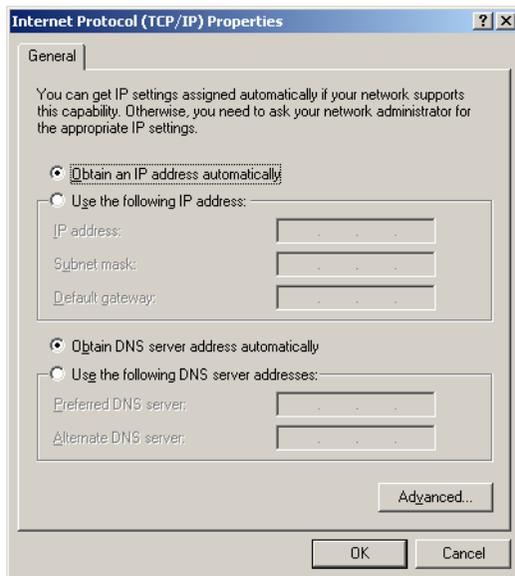
4 Click **Properties**.

The network connection Properties dialog box appears.



5 Double click the **Internet Protocol (TCP/IP)** component.

The Internet Protocol (TCP/IP) Properties dialog box appears.



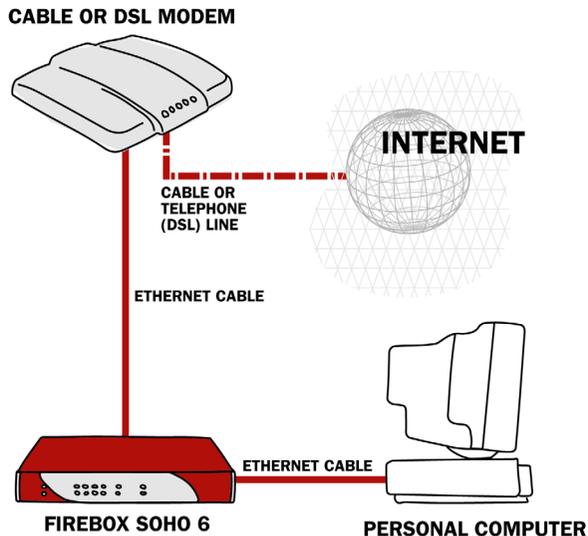
- 6 Select **Obtain an IP address automatically**. Select **Obtain DNS server address automatically**.
- 7 Click **OK** to close the Internet Protocol (TCP/IP) Properties dialog box. Click **OK** again to close the network connection Properties dialog box. Click **Close** to close the network connection dialog box. Close the Control Panel window.

Physically connect the SOHO 6

Your SOHO 6 protects a single computer or a multi-computer network. It also functions as a hub to connect a variety of other appliances.

Cabling the SOHO 6 for one to four appliances

Each of the Trusted Network ports (numbered 0-3) is able to connect to a variety of appliances. These include computers, printers, scanners, or other network peripherals. Use your SOHO 6 to replace an existing hub if you have no more than four appliances to connect.



- 1 Shut down your computer. If you connect to the Internet using a DSL/cable modem, disconnect the power from this device
- 2 Disconnect the Ethernet cable that runs from your DSL/cable modem or other Internet connection to your computer and connect it to the WAN port on the SOHO 6.
The SOHO 6 is now connected directly to the modem or other Internet connection.
- 3 Connect one end of the straight-through Ethernet cable supplied with your SOHO 6 into any one of the four,

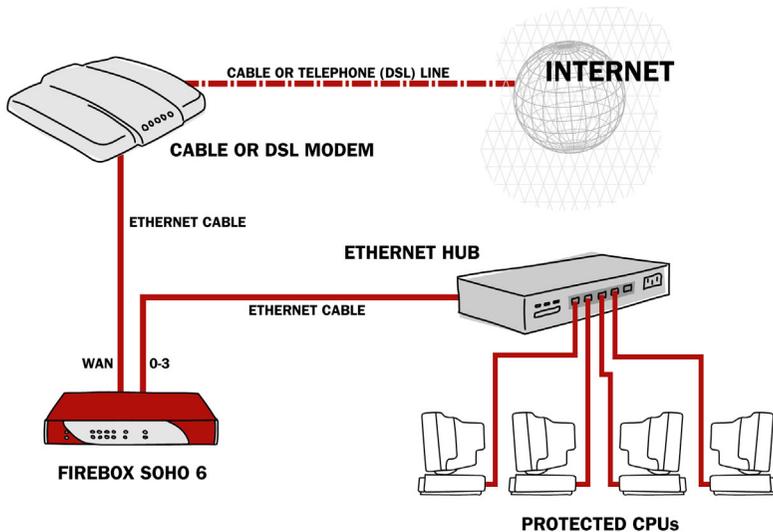
numbered, Ethernet ports (labeled 0-3) on the SOHO 6. Connect the other end into the Ethernet port of your computer. The SOHO 6 is now connected to the Internet and your computer.

- 4 If you connect to the Internet using a DSL/cable modem, restore the power to this device. When the indicator lights of the modem stop flashing the modem is ready for use.
- 5 Attach the AC adapter to the SOHO 6 and connect it to a power source.
- 6 Restart your computer.

For information on the factory default configuration options, see “Default Factory Settings” on page 25. For specialized configurations, see “Configure Your External Network” on page 31, as well as, “Configure the Trusted Network” on page 36.

Cabling the SOHO 6 for more than four computers

While there are only four, numbered, Ethernet ports (labeled 0-3) on the back of the SOHO 6, it is possible to connect more appliances to your SOHO 6 using network hubs.



The SOHO 6 ships with a “10-seat” license. In other words, the SOHO 6 allows up to ten computers on a network behind the SOHO 6 to access the Internet. More than ten computers can exist on the network and communicate with each other, but only the first ten that attempt to access the Internet are allowed through the SOHO 6. A seat is taken when a computer connects to the Internet. To upgrade your SOHO 6 user license, please visit:

<http://www.watchguard.com/sales/buyonline.asp>

You need these additional items:

- One or more Ethernet hubs.
- An Ethernet cable (with RJ-45 connectors) for each computer to connect to the SOHO 6.
- An Ethernet cable to connect each hub to the SOHO 6.

- 1 Shut down your computer. If you connect to the Internet using a DSL/cable modem, disconnect the power from this device

- 2 Disconnect the Ethernet cable that runs from your DSL/cable modem or other Internet connection to your computer and connect it to the WAN port on the SOHO 6.

The SOHO 6 is now connected directly to the modem or other Internet connection.

- 3 Connect one end of the straight-through Ethernet cable supplied with your SOHO 6 into any one of the four, numbered, Ethernet ports (labeled 0-3) on the SOHO 6. Connect the other end into the uplink port of the hub.

The SOHO 6 is now connected to the Internet and your hub.

- 4 Connect Ethernet cables to the uplink ports of the hub and to the Ethernet ports of each of your computers.

- 5 If you connect to the Internet using a DSL/cable modem, restore the power to this device. When the indicator lights of the modem stop flashing the modem is ready for use.

- 6 Attach the AC adapter to the SOHO 6 and connect it to a power source.

- 7 Restart your computer.

For information on the factory default configuration options, see “Default Factory Settings” on page 25. For specialized configurations, see “Configure Your External Network” on page 31, as well as, “Configure the Trusted Network” on page 36.

Once you have physically installed the SOHO 6, you can connect to it using your Web browser. The SOHO 6 includes a Web server that provides a configuration, Web page interface.

The SOHO 6 Home Page—System Status

With your Web browser, go to the System Status page of the SOHO 6 using the default IP address of the Trusted Network:

<http://192.168.111.1>.

The System Status page appears.

System Status

Welcome to the SOHO configuration site. The standard configuration provides basic protection against network security attacks. Through this site you can customize the SOHO to meet your specific security needs.

If you need assistance, click [Help](#) for information about what each of the configuration options mean.

Component	Version	Feature	Status	
Firewall	6.1.34	WSEP Logging	Disabled	Configure
	Dec 10 2002	VPN Manager Access	Disabled	Configure
BootROM	4.14	Syslog	Disabled	Configure
Platform	WatchGuard SOHO 6 TC	Pass Through	Disabled	Configure
Serial Number	6062015884062			
		Option	Status	
		User Licenses	10	Upgrade
		Managed VPN	Disabled	Configure
		Manual VPN	0 configured (max 6)	Configure
		MUVPN Clients	Not Installed	Upgrade
		WebBlocker	Disabled	Configure
		Dual ISP	Not Installed	Upgrade
		VPNforce	Not Installed	Upgrade

[Reboot](#) [Update](#)

The System Status page is effectively the home page of the SOHO 6. A variety of information is revealed in an effort to provide a comprehensive display of the SOHO 6 configuration. This information includes:

- The firmware version
- The serial number of the appliance
- A few of the SOHO 6 features and their status:
 - WSEP Logging
 - VPN Manager Access
 - Syslog

- Pass Through
- Upgrade options and their status
- Configuration information for both the Trusted and External networks

NOTE

When the External network is configured to use the PPPoE Client, the page also displays a connect or disconnect button in order to terminate or initiate the PPPoE connection.

- Configuration information on firewall settings (Incoming and Outgoing services)
- A reboot button to restart the SOHO 6

Default Factory Settings

Your SOHO 6 has the following default network and configuration settings:

External Network

External network settings use DHCP.

Trusted Network

The trusted network IP address is 192.168.111.1.

All computers on the trusted network automatically receive their addresses using DHCP.

Firewall Settings

- All incoming services are blocked.
- An outgoing service allowing all outbound traffic.
- None of the Firewall Options are enabled.
- The DMZ pass-through is disabled.

System Security

- System Security is disabled and no System Administrator name or passphrase is set—the configuration pages are available to all on the trusted network.
- SOHO 6 Remote Management is disabled.
- VPN Manager Access is disabled.
- No remote logging is configured.

WebBlocker

- WebBlocker is disabled and no settings are configured.

Upgrade Options

- No upgrade options are enabled until the license keys are redeemed.

Reset a SOHO 6 to factory default

Firmware corruptions or other unforeseen events (such as a lost System Security passphrase) require you to reset the SOHO 6 to its factory default settings.

To do this, first disconnect the power supply. Then find the reset button located at the rear of the SOHO 6. Press and hold the reset button. At the same time, reconnect the power supply. Continue pressing the reset button while the SOHO 6 reboots—approximately 15 seconds. The PWR indicator light should blink in a steady pattern once the reboot is complete. When this occurs, reboot the SOHO 6 again by disconnecting the power supply.

Finally, the PWR indicator light should remain illuminated. Your SOHO 6 is now reset to factory defaults.

The base model SOHO 6

The base model SOHO 6 comes with a ten-seat license; that is, ten computers have access to the Internet through the SOHO 6. Remember, while only four appliances connect directly to the four (numbered 0-3) Ethernet ports, one or more of these appliances can be a hub or router. Please see, “Cabling the SOHO 6 for more than four computers” on page 20.

Register your SOHO 6 and Activate the LiveSecurity Service

Once the SOHO 6 is installed and configured, you need to register the unit and activate your bundled LiveSecurity Service subscription. Activation entitles you to receive threat alert notifications, expert security advice, free anti-virus protection, software updates, technical support by web or phone, and access to extensive online help resources and our user forum. You must also activate to retrieve feature keys for any upgrades you have purchased.

Be sure that you have the SOHO 6 serial number handy. You will need this during the registration process.

To register with the LiveSecurity Service:

- 1 Using your Web browser, go to:
<http://www.watchguard.com/activate>

NOTE

You *must* have JavaScript enabled on your browser to be able to activate LiveSecurity Service.

If you are a returning customer, log in with your user name and password then choose your product and continue by following the instructions on screen.

If you are a new WatchGuard customer, begin by creating a profile, then follow the instructions on screen for activating a product.

Please use the table below to record your LiveSecurity Service identification information:

Serial Number:	
LiveSecurity User Name:	
Password:	

The SOHO 6 serial number is located on the bottom of the appliance. You create a LiveSecurity Service user name and password when you register your SOHO 6.

Please keep this information in a secure place.

Reboot the SOHO 6

To reboot a SOHO 6 located on a local system, use one of these methods:

- With your Web browser, go to the System Status page using the trusted IP address of the SOHO 6. For example, if using

the default IP address, go to: <http://192.168.111.1>. Click **Reboot**.

- Unplug the SOHO 6 and reconnect it to a power source.

To reboot a SOHO 6 located on a remote system, you must set the SOHO 6 to allow either incoming HTTP (Web) or FTP traffic to the trusted address of the SOHO 6. For information on configuring a SOHO 6 to allow incoming traffic, see “Configure Incoming and Outgoing Services” on page 62.

You then use one of these methods:

- With your Web browser, go to the System Status page using the external IP address of the SOHO 6. Click **Reboot**.
- Send an FTP command to the remote SOHO 6. Use an FTP application to connect to the SOHO 6, then enter the command: `quote rebt`

Configure the Network Interfaces

Configure Your External Network

When you configure the external network, you establish how the SOHO 6 communicates with your ISP. This configuration depends upon how your ISP distributes network addresses—using DHCP or PPPoE.

Network addressing

Each networked computer must have an IP address to identify itself to other computers. IP address assignments are either dynamic or static. With a dynamic IP address, your ISP assigns each computer a different address each time it connects to the server. When you power down the computer, you release that IP address allowing it to be reassigned. A static IP address is assigned to your computer at all times whether or not you are currently using it. No other computer on the network shares that address.

The most common method to distribute IP addresses is dynamically using DHCP (Dynamic Host Configuration Protocol). When your computer is connected to the network, a DHCP server at your ISP automatically assigns it a network IP address. This relieves the ISP of the responsibility to manually assign and manage individual IP addresses.

Another method of dynamically assigning IP addresses is called PPPoE (Point-to-Point Protocol over Ethernet). PPPoE combines some of the advantages of Ethernet and PPP by simulating a standard dial-up connection. It is popular among many ISPs because it allows them to use their existing dial-up infrastructure such as billing, authentication, and security for DSL and cable modems. When configured to use PPPoE, the connection can be manually connected or disconnected from the System Status page.

Contact your ISP to determine which method they use to assign your IP address.

Configure the SOHO 6 External Network for dynamic addressing

The SOHO 6 is configured to obtain its external address information automatically using DHCP. If your ISP supports this method, the SOHO 6 obtains all necessary address information when it powers on and attempts to connect to the Internet. No further configuration of the SOHO 6 is required.

Configure the SOHO 6 External Network for static addressing

If you are assigned a static address, then you must transfer the permanent address assignment from your computer to the SOHO 6. Instead of communicating directly to your computer, the ISP now communicates through the SOHO 6.

- 1 With your Web browser, go to the System Status page using the trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: <http://192.168.111.1>
- 2 From the navigation bar on the left side, select **Network** ⇒ **External**.
The External Network Configuration page appears.
- 3 From the Configuration Mode drop list, select **Manual Configuration**.
The page refreshes.

System Status Network External Trusted Optional Routes Dual ISP Network Statistics DynamicDNS Administration System Security VPN Manager Access Update Upgrade View Configuration File Firewall Incoming Outgoing	<p style="text-align: center;"><u>Network</u></p> <h3 style="text-align: center;">External Network Configuration</h3> <hr/> <p>Configuration Mode <input type="text" value="Manual Configuration"/></p> <p>IP Address <input type="text" value="0.0.0.0"/></p> <p>Subnet Mask <input type="text" value="255.255.255.0"/></p> <p>Default Gateway <input type="text" value="0.0.0.0"/></p> <p>Primary DNS <input type="text" value="66.235.63.2"/></p> <p>Secondary DNS <input type="text" value="66.235.63.4"/></p> <p>DNS Domain Suffix <input type="text"/></p> <hr/> <p style="text-align: center;"> <input type="button" value="Submit"/> <input type="button" value="Reset"/> </p>
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

- 4 Enter the TCP/IP settings you recorded from your computer during the installation process. Refer to the table in, “Review and record your current TCP/IP settings” on page 12.
- 5 Click **Submit**.
The configuration change is saved to the SOHO 6.

Configure the SOHO 6 External Network for PPPoE

While less common, PPPoE is another method for an ISP to assign IP addresses. Check the information and manuals sent to you by your ISP to see if they use PPPoE. If you cannot find this information, contact your ISP and ask them. You need your PPPoE login name and password.

To configure the SOHO 6 for PPPoE:

- 1 Open your Web browser and click **Stop**.
At this point, the Internet connection is not fully configured, and the computer cannot load your home page from the Internet. However, the computer can access the configuration Web pages installed on the SOHO 6.
- 2 With your Web browser, go to the System Status page using the trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: <http://192.168.111.1>
- 3 From the navigation bar on the left side, select **Network** ⇒ **External**.
The External Network configuration page appears.

- From the Configuration Mode drop list, select **PPPoE Client**. The page refreshes.

System Status

Network

- External
- Trusted
- Optional
- Routes
- Dual ISP
- Network Statistics
- DynamicDNS

Administration

- System Security
- VPN Manager Access
- Update
- Upgrade
- View Configuration File

Firewall

- Incoming

Network

External Network Configuration

Configuration Mode: PPPoE Client

Name:

Domain:

Password:

Inactivity Timeout (minutes):

Automatically restore lost connections

Enable pppoe debug trace

- Enter the PPPoE login name and domain supplied by your ISP.
- Enter the PPPoE password supplied by your ISP.
- Enter how long you want the system to wait before it disables an inactive TCP connections.
- Click **Automatically restore lost connections**.
This enables a constant flow of "heartbeat" traffic between the SOHO 6 and the PPPoE server. In the event of routine packet loss, this option allows the SOHO 6 to maintain the PPPoE connection. The SOHO 6 may reboot to recover this connection if the heartbeat fails. This provides for a more consistent Internet connection and is seen as continuous traffic by the ISP and regulated (and in some cases billed) as such. This option is also used for Technical Support debugging purposes.
- Click **Enable pppoe debug trace** to activate PPPoE debug trace.
- Click **Submit**.
The configuration change is saved to the SOHO 6.

Configure the Trusted Network

By default, the SOHO 6 uses DHCP to assign addresses to computers on your trusted network. In other words, every time you connect a computer to the SOHO 6, either directly or through a hub, it automatically attempts to obtain its addresses from the SOHO 6. If you use a centralized DHCP server to hand out IP addresses, the SOHO 6 has a DHCP Relay feature that forwards the DHCP request to the specified DHCP server.

Configure DHCP Server and DHCP Relay

To configure DHCP server:

- 1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: <http://192.168.111.1>
- 2 From the navigation bar on the left side, select **Network** ⇒ **Trusted**.

The Trusted Network Configuration page appears.

- 3 Enter the IP address and the Subnet Mask in the appropriate fields.
- 4 Enable the checkbox labeled **Enable DHCP Server on the Trusted Network**.
- 5 Enter the first IP address the DHCP server will hand out to computers connect to the Trusted network.
- 6 Enter the WINS Server address, DNS Server address (primary and secondary), and DNS Domain server suffix.
- 7 Click **Submit** and reboot the SOHO 6 as necessary.

To configure the DHCP Relay Server:

- 1 From the Trusted Network Configuration page, enable the checkbox labeled **Enable DHCP Relay**.

- 2 Enter the IP address of the DHCP relay server.
- 3 Click **Submit** and reboot the SOHO 6 as necessary.

The SOHO 6 will now send all DHCP requests to the specified, remote DHCP server and relay the resulting IP addresses to the computers connected to the Trusted Network. If the SOHO 6 is unable to contact the specified, remote DHCP server in 30 second, it will revert to using its own DHCP server to respond to computer on the Trusted network.

Configure additional computers on the Trusted Network

The SOHO 6 accepts connections from up to four computers. Network a larger number of computers together using one or more 10BaseT Ethernet hubs with RJ-45 connectors. The SOHO 6 system coexists with other systems over the same LAN (Local Area Network). If you mix computers with different operating systems on your network they pass traffic through the SOHO 6 to access the Internet.

Follow these steps to add one or more computers to your Trusted network:

- 1 Verify that each additional computer has an Ethernet card installed. Shut the computer down, connect it to the network the same way you did in “Cabling the SOHO 6 for more than four computers” on page 20. Restart the computer.
- 2 Set the computers to obtain their addresses using DHCP. For instructions see, “Enable your computer for DHCP” on page 16.
- 3 Turn off and restart each computer.

Configure the Trusted Network with static addresses

To disable the SOHO 6 DHCP server and assign addresses statically, follow these steps:

- 1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: <http://192.168.111.1>
- 2 From the navigation bar on the left side, select **Network** ⇒ **Trusted**.
The Trusted Network Configuration page appears.

System Status

Network

- External
- Trusted**
- Optional
- Routes
- Network Statistics
- DynamicDNS

Administration

- System Security
- VPN Manager Access
- Update
- Upgrade
- View Configuration File

Firewall

- Incoming
- Outgoing
- Custom Service
- Blocked Sites
- Firewall Options
- Pass Through

Logging

Network

Trusted Network Configuration

IP Address

Subnet Mask

Enable DHCP Server on Trusted Network

First address for DHCP server

WINS Server Address

DNS Server Address

Secondary DNS Server Address

DNS Domain Suffix

Enable DHCP Relay

DHCP relay server

- 3 Enter the IP address and the Subnet Mask in the appropriate fields.

- 4 Disable the checkbox labeled **Enable DHCP Server on the Trusted Network**.
- 5 Click **Submit** and reboot the SOHO 6 as necessary.
- 6 Configure your computers and other devices on the trusted network with static addresses.

Configure Static Routes

The SOHO 6 allows you to configure static routes in order to pass traffic to networks on separate segments. This means that the SOHO 6 can route data packets to additional networks connected to a router or switch behind the SOHO 6.

Follow these instructions to configure static routes:

- 1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: <http://192.168.111.1>
- 2 From the navigation bar on the left side, select **Network ⇒ Routes**.

The Routes page appears.

The screenshot shows a web interface with a left-hand navigation menu and a main content area. The navigation menu includes sections for System Status, Network, Administration, and Firewall. The 'Routes' option under the Network section is highlighted. The main content area is titled 'Network Routes' and contains a table with two columns: 'Address' and 'Gateway'. Below the table are two buttons: 'Add...' and 'Remove'.

3 Click **Add**.

The Add Route page appears.

The screenshot shows the 'Add Route' page. The navigation menu is on the left, and the main content area is titled 'Network > Routes Add Route'. It features a 'Type' dropdown menu set to 'Host', and two text input fields for 'Address' and 'Gateway'. At the bottom, there are three buttons: 'Submit', 'Reset', and 'Cancel'.

4 From the Type drop list, select either **Host** or **Network**.

5 Enter the IP address and the Gateway of the route in the appropriate field.

The gateway of the route is the local interface of the router.

6 Click **Submit**.

To remove a route, select the appropriate entry and click **Remove**.

View Network Statistics

The SOHO 6 has a configuration page that displays a variety of network statistics to assist in monitoring data traffic as well as troubleshooting potential problems.

Follow these instructions to view this page:

1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.

For example, if using the default IP address, go to: <http://192.168.111.1>

2 From the navigation bar on the left side, select **Network => Network Statistics**.

The Network Statistics page appears.

The screenshot shows the 'Network Statistics' page. On the left is a navigation sidebar with the following items: System Status, Network (selected), External, Trusted, Optional, Routes, Dual ISP, Network Statistics (highlighted), DynamicDNS, Administration, System Security, VPN Manager Access, Update, Upgrade, View Configuration File, Firewall, Incoming, Outgoing, Custom Service, Blocked Sites, Firewall Options, and Pass Through. The main content area is titled 'Network Statistics' and is divided into three sections: 'IP', 'External Network', and 'Trusted Network'. The 'IP' section shows the IP is 'Up for 1 hour 26 seconds' and lists various network metrics. The 'External Network' section shows statistics for the 'eth0' interface. The 'Trusted Network' section is currently empty.

Section	Statistics
IP	IP: Up for 1 hour 26 seconds Network Buffers Allocated/Total (2/40) Memory Total/Largest Block (10764224/1062771) Sockets Allocated/Total (12/80) NAT Ports Avail (1000)RAM Disk (56880) Tx: packets (7136) Rx: packets (8049) hdr Err(87) delivered (3851) forward (4111)
External Network	eth0: Link encap:Ethernet HWaddr 00:90:7f:12:75:39 inet addr:66.235.9.181 RX packets:2346 errors:0 bcast:43004 disc:0 unk:11293 TX packets:1825 errors:0 bcast:2
Trusted Network	

Configure the Dynamic DNS Service

This feature allows you to register the external, IP address of the SOHO 6 with a dynamic DNS (Domain Name Server) service (www.dyndns.org). This service allows customers to bind their DNS record in the event that their dynamically assigned IP address is reassigned.

- 1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: <http://192.168.111.1>

NOTE

WatchGuard is not affiliated with dyndns.org.

- 2 From the navigation bar on the left side, select **Network** ⇒ **DynamicDNS**.
The Dynamic DNS client page appears.

The screenshot shows the configuration interface for Dynamic DNS. On the left, a navigation menu lists various system settings, with 'DynamicDNS' highlighted under the 'Network' category. The main panel, titled 'Network Dynamic DNS client', features a checkbox to 'Enable Dynamic DNS client'. Below this are three text input fields labeled 'Domain', 'Name', and 'Password'. At the bottom of the panel are 'Submit' and 'Reset' buttons.

- 3 Select the **Enable Dynamic DNS client** checkbox.
- 4 Enter the domain, name, and password in the appropriate fields.

NOTE

The SOHO 6 receives the IP of members.dyndns.org when it connects to the time server.

5 Click **Submit**.

Configure OPT Port Upgrades

The optional port, OPT port, on the SOHO 6 supports two new upgrades:

- Dual ISP Port upgrade
- VPNforce Port upgrade

To activate these upgrades, you need to buy an additional license, and then Upgrade the SOHO 6 to activate the new feature. For more information on how to Upgrade the SOHO 6,, see “Redeem your SOHO 6 Upgrade Options” on page 57.

NOTE

The OPT port is only available if you purchase a software upgrades. You can not use the OPT port as another internet port on the Trusted network.

Configure Dual ISP Port

The Dual ISP Port upgrade adds fail-over support for the External interface. This means that when the primary external port connections fails, the firewall will initiate a connection through the optional port.

No new policy definitions are needed. The optional port uses the same set of policies as the external port.

The SOHO 6 uses two methods to determine if the external port connection is down:

- The link to the nearest router
- A ping to a specified location.

The SOHO pings the default gateway or other location designated by the administrator. If there is no response, fail-over takes place.

When this feature is activated, these actions automatically occur:

- If the external port (EXT) connection fails, the optional port (OPT) connection is initiated and used
- If the optional port (OPT) connection fails the external port (EXT) connection is opened and used
- If both connections fail the SOHO 6 repeatedly tries both external and optional ports until a connection is made

There is no automatic return to the external port (EXT) if this port comes back online unless you use PPPoE to assign IP addresses. Once the fail-over has switched to the optional port (OPT), the administrator has to change the configuration back to the external port (EXT) when it comes back online.

If you use PPPoE, you can set an inactivity timeout, which disables any inactive TCP connections until traffic resumes. For information on setting up PPPoE, see “Configure the SOHO 6 External Network for PPPoE” on page 34. If your external port (EXT) connection fails, the optional port (OPT) connection is initiated and used. The optional port (OPT) stays connected until the TCP connection is not active (timeout). When traffic resumes, the SOHO attempts to connect with the external port (EXT) first. If this connection is active, the external port (EXT) becomes the active port again. If the external port (EXT) is still unavailable, the SOHO attempts to connect with the optional port (OPT).

Once you have upgraded to the SOHO 6 to activate this features, follow these instructions to configure Dual ISP Port:

- 1 Connect one end of a straight-through Ethernet cable into the OPT port, and connect the other end into the source of the secondary or fail-over External network connection. This can be either a DSL/cable modem or Hub.
- 2 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.

For example, if using the default IP address, go to: <http://192.168.111.1>

- 3 From the navigation bar on the left side, select **Network** ⇒ **Dual ISP**.

The Dual ISP Options page appears.

The screenshot shows the 'Dual ISP Options' configuration page. On the left is a navigation menu with categories: System Status, Network, Administration, and Firewall. Under 'Network', 'Dual ISP' is selected. The main content area is titled 'Network Dual ISP Options' and contains the following settings:

- Enable Dual ISP
- Host to ping on External:
- Host to ping on Optional:
- Ping interval (in seconds):
- Reply Timeout (in seconds):
- No reply limit:

At the bottom of the form are two buttons: 'Submit' and 'Reset'.

- 4 Select the **Enable Dual ISP** checkbox.
- 5 Enter the IP address for the External Interface.
- 6 Enter the IP address for the Optional or Failover Interface.
- 7 Enter how many seconds between pings.
- 8 Enter how long (in seconds) to wait for a reply.

- 9 Enter the number of times the system will ping the Interface before timeout.
- 10 Click **Submit**.

Configure VPNforce™ Port

The VPNforce port upgrade activates the SOHO 6 optional port for use on the trusted side. It's main function is to provide a remote office or telecommuter a separate network behind the SOHO 6 firewall; one with secure access to the corporate network while the other connection is used for non-corporate functions.

When the optional port is activated with this upgrade a separate subnet is defined that is distinct from that used by the Trusted ports. By default, the subnet for the optional port is 192.168.112.0.

Once you have upgraded to the SOHO 6 to activate this feature, follow these instructions to configure VPNforce Port:

- 1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: <http://192.168.111.1>

- From the navigation bar on the left side, select **Network** ⇒ **Optional**.

The Optional Network Configuration page appears.

The screenshot shows the 'Optional Network Configuration' page. On the left is a navigation menu with categories: System Status, Network (selected), Administration, Firewall, Logging, WebBlocker, and VPN. Under 'Network', 'Optional' is highlighted. The main area has the title 'Optional Network Configuration' and the following settings:

- Enable Optional Network
 - IP Address:
 - Subnet Mask:
- Enable DHCP Server on Optional Network
 - First address for DHCP server:
 - WINS Server Address:
 - DNS Server Address:
 - Secondary DNS Server Address:
 - DNS Domain Suffix:
- Enable DHCP Relay on Optional Network
 - DHCP relay server:
- Allow traffic between Optional Network and Trusted Network
- Require encrypted MUVPN connections on this interface

At the bottom are 'Submit' and 'Reset' buttons.

- To enable VPNforce, select the **Enable Optional Network** checkbox.
- Enter the configuration information (IP address, DHCP Server, and DHCP Relay) for the Optional Interface, which is the same process as configuring the Trusted network. For specific instructions on these fields, see “Configure the Trusted Network” on page 36.
- To allow traffic between the Optional and Trusted network, enable the **Allow traffic between Optional Network and Trusted Network** checkbox.

- 6 To require encrypted MUVPN connections on this interface, enable the **Require Encrypted MUVPN connections on this interface** checkbox.
- 7 Click **Submit**.

Administrative Options

The SOHO 6 Administration page is where you configure access to the SOHO 6—using System Security, enabling SOHO 6 Remote Management, or providing VPN Manager Access. You can also update the firmware, enter the feature key for any upgrade options you have purchased and have redeemed at the LiveSecurity Service Web site, as well as see the SOHO 6 configuration file in a text format.

The System Security Page

The System Security configuration page allows you to create secure settings to protect the configuration of the SOHO 6. Setting a system administrator name and system passphrase allows you to protect the SOHO 6 by using a simple authentication method.

This page also allows you to create a secure connection, using IPsec (Internet Protocol Security), to the SOHO 6 from a remote location.

System management

Passphrases are a barrier between your computer and anyone trying to break in. They are the first line of defense in computer security. They are, unfortunately, the most frequently overlooked of all security measures. The SOHO 6 system administrator name and system passphrase are designed to protect the SOHO 6 configuration from alteration by someone on your trusted network. In other words, when you configure a SOHO 6 system administrator name and system passphrase, no one in your office is able to change (deliberately or accidentally) your firewall settings without the proper passphrase.

NOTE

Make certain that you do not lose this name and passphrase. Once system security protection is activated, there is no other means of accessing your SOHO 6 settings. Should you forget your name or passphrase, the only means of accessing the appliance requires reverting your SOHO 6 to its factory settings; see "Reset a SOHO 6 to factory default" on page 26, you will then need to reconfigure your SOHO 6.

Change the system passphrase at least monthly. A passphrase (eight characters long) is a combination of letters, numbers, and symbols that do not spell out common words. WatchGuard

recommends that the passphrase contain at least one special character, number, and a mixture of upper and lower case letters for increased security.

Follow these steps to setup the SOHO 6 System Passphrase:

- 1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: `http://192.168.111.1`.
- 2 From the navigation bar on the left side, select **Administration** ⇒ **System Security**.
The System Security page appears.

System Status Network External Trusted Optional Routes Network Statistics DynamicDNS Administration System Security VPN Manager Access Update Upgrade View Configuration File Firewall Incoming Outgoing Custom Service Blocked Sites Firewall Options Pass Through Logging WSEP Logging	<div style="text-align: right;"> Administration System Security </div> <hr/> HTTP Server Port <input type="text" value="80"/> <input type="checkbox"/> Enable System Security System Administrator Name <input type="text"/> System Passphrase <input type="text"/> Confirm System Passphrase <input type="text"/> <input type="checkbox"/> Enable SOHO Remote Management Virtual IP Address <input type="text" value="0.0.0.0"/> Authentication Algorithm <input type="text" value="MD5-HMAC"/> Encryption Algorithm <input type="text" value="DES-CBC"/> VPN Client Type <input type="text" value="Mobile User"/> <hr/> <input type="button" value="Submit"/> <input type="button" value="Reset"/>
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

- 3 Verify that the HTTP Server Port is set at 80.
- 4 Select the **System Security** checkbox.

- 5 Enter the System Administrator Name.
- 6 Enter the System Passphrase and confirm it.
- 7 Click **Submit**.

SOHO Remote Management

This page also allows you to create a secure connection, using Internet Protocol Security (IPSec), to the SOHO from a remote location: SOHO Remote Management. This feature is discussed at length in the *Firebox SOHO 6 Remote Management Guide* located on our Web site at:

<http://help.watchguard.com/documentation/soho.asp>

Set up VPN Manager Access

The SOHO 6 works with WatchGuard VPN Manager software access in order to configure and manage Branch Office VPN tunnels from a remote location.

VPN Manager software is purchased separately and must run on a WatchGuard Firebox II/III. For more information regarding the VPN Manager product, use your Web browser to go to:

<https://www.watchguard.com/products/vpnmanager.asp>

Follow these steps to setup VPN Manager access:

- 1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: <http://192.168.111.1>

- From the navigation bar on the left side, select **Administration** ⇒ **VPN Manager Access**.
The VPN Manager Access page appears.

The screenshot shows a web interface for configuring VPN Manager Access. On the left is a dark navigation menu with the following items: System Status, Network (External, Trusted, Optional, Routes, Network Statistics, DynamicDNS), Administration (System Security, VPN Manager Access, Update, Upgrade, View Configuration File), and Firewall. The 'VPN Manager Access' item is highlighted. The main content area has a title 'Administration' and a sub-title 'VPN Manager Access'. Below the title is a horizontal line. Underneath is a checkbox labeled 'Enable VPN Manager Access'. To the right of the checkbox are four text input fields: 'Status Passphrase', 'Confirm Status Passphrase', 'Configuration Passphrase', and 'Confirm Configuration Passphrase'. At the bottom of the form are two buttons: 'Submit' and 'Reset'.

- Select **Enable VPN Manager Access**.
- Enter the status passphrase and confirm it.
- Enter the configuration passphrase and confirm it.

NOTE

These two settings *must* exactly match the passphrases used in the VPN Manager or the connection will fail.

- Click **Submit**.

Update Your Firmware

As new firmware is released, you should update the version running on your SOHO 6. New updates are located on the WatchGuard Web site at:

<http://support.watchguard.com/sohoresources/>

Download the new firmware file from the Web site and save it to a known location on your management station.

Once you have downloaded the firmware, follow these steps to update the version running on your SOHO 6:

- 1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: <http://192.168.111.1>
- 2 From the navigation bar on the left side, select **Administration** ⇒ **Update**.
The Update page appears.

NOTE

If you are managing your SOHO 6 from a computer running an operating system other than Windows (such as a Macintosh or Linux OS), you *must* update your firmware from this configuration page as firmware versions are released. This is because WatchGuard installation applications are only built for Windows platforms.

- 3 Read through the End-User License Agreement, then select the **I accept the above license agreement** checkbox at the bottom of the page.

I accept the above license agreement.

Select file

- 4 Enter the location of the firmware files located on your computer.
- 5 If you do not know the location of the firmware files, click **Browse** to browse your computer's directories and select them.
- 6 Click **Update**.
Follow the instructions provided by the Update Wizard.

NOTE

The Update Wizard will request a User name and Password. These values correspond System Administrator Name and System Passphrase configured at the System Security page. The default values are User and Pass.

Redeem your SOHO 6 Upgrade Options

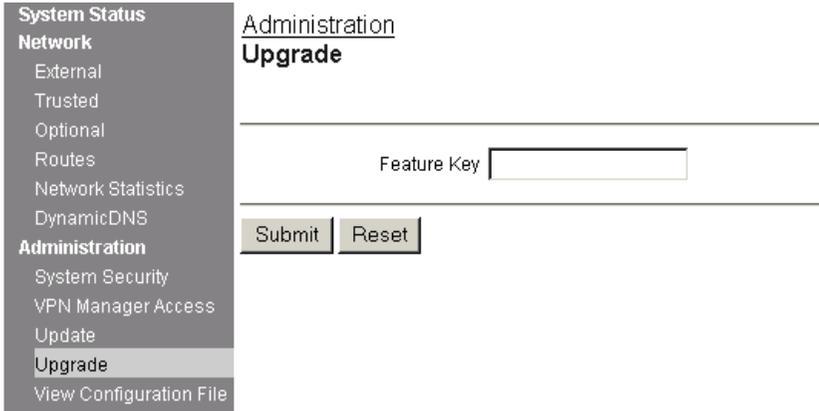
When you purchase a SOHO 6, the software for all upgrade options is provided with the unit regardless of whether you have actually purchased any of those options. The Feature Key that enables these software options is stored within the SOHO 6. Once you purchase an upgrade option and redeem it at the LiveSecurity Service Web site, you will receive a Feature Key, which you can then copy and paste into a SOHO 6 configuration page, to activate the software upgrade.

For information on registering your SOHO 6 with the LiveSecurity Service, see "Register your SOHO 6 and Activate the LiveSecurity Service" on page 27.

Follow these steps to redeem your upgrade option license key:

- 1 With your Web browser, go to:
<http://www.watchguard.com/upgrade>
- 2 Log into the site by entering your **User Name** and **Password**.

- 3 Follow the instructions provided on the site to redeem your upgrade license key.
- 4 Copy the Feature Key displayed at the LiveSecurity Service Web site.
- 5 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: <http://192.168.111.1>
- 6 From the navigation bar on the left side, select **Administration =>Upgrade**.
The Upgrade page appears.



- 7 Paste the Feature Key in the appropriate field.
- 8 Click **Submit**.

Upgrade options

Seat Licenses

This upgrade to the SOHO 6 provides more seats than the base model offers (for example, the 25 seat license).

Dual ISP Port

This upgrade to the SOHO 6 activates the Optional port as a fail-over support for the external interface. This license key is purchased separately.

VPNforce Port

This upgrade to the SOHO 6 activates the Optional port as a separate secure connection to a corporate network for a remote office or telecommuter. This license key is purchased separately.

IPSec Virtual Private Networking (VPN)

The SOHO 6tc comes with a VPN upgrade license key. You must activate the VPN upgrade in order to configure virtual private networking. The SOHO 6 does not come with the VPN upgrade license key. This license key is purchased separately.

WebBlocker

The SOHO 6 has a Web filtering option. This license key is purchased separately.

MUVPN Clients

With this upgrade the SOHO 6 allows remote users to securely connect to it through an IPSec VPN and access network resources on the Trusted network. These license keys are purchased separately.

LiveSecurity Service Subscription Renewals

Subscription renewals are available for a period of one or two years and may be purchased from your reseller or from the WatchGuard online store. To purchase renewals online or activate a renewal certificate, visit:

<http://www.watchguard.com/renew/>

Follow the instructions at the site to activate or purchase the renewal.

View the Configuration File

From this configuration page, the SOHO 6 configuration file appears in text format.

- 1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: <http://192.168.111.1>
- 2 From the navigation bar on the left side, select **Administration** ⇒ **View Configuration File**.
The View Configuration File page appears.

Configure the Firewall Settings

Firewall Settings

The flow of incoming and outgoing traffic is controlled by the configuration setting you make. These decisions are made in accordance with a sound security policy that defines the kinds of risks that are acceptable to you or your firm.

WatchGuard identifies several commonly used services that are used to define incoming and outgoing access. A service is the combination of protocol and port numbers associated with a specific application or communication type.

Configure Incoming and Outgoing Services

By default, the security stance of the SOHO 6 is to deny incoming packets to computers on the trusted network protected by the SOHO 6 firewall. You can selectively open your network to certain types of Internet connectivity. For example, to set up a Web server behind the SOHO 6, you add an incoming Web service.

It is important to remember that each service you add opens a small window into your trusted network and marginally reduces your security. This is the inherent trade-off between access and security.

Pre-configured Services

Each service is defined by a combination of Internet protocols and port numbers to uniquely identify the connection type to applications and servers on the Internet. The SOHO 6 configuration pages include several of the most common types.

Follow these steps to add an Incoming service:

- 1 From the navigation bar on the left side, select **Firewall ⇒ Incoming** or **Outgoing**.
The Filter Traffic page appears.

System Status

Network

External

Trusted

Optional

Routes

Network Statistics

DynamicDNS

Administration

System Security

VPN Manager Access

Update

Upgrade

View Configuration File

Firewall

Incoming

Outgoing

Custom Service

Blocked Sites

Firewall

Filter Incoming Traffic

Common Services

Filter		Service	Service Host
No Rule		CU-SeeMe	0.0.0.0
No Rule		DNS	0.0.0.0
No Rule		FTP	0.0.0.0
No Rule		HTTP	0.0.0.0
No Rule		HTTPS	0.0.0.0
No Rule		ILS	0.0.0.0
No Rule		IPSec	0.0.0.0
No Rule		NetMeeting	0.0.0.0
No Rule		NNTP	0.0.0.0

- 2 Locate a pre-configured service, such as FTP, Web, or Telnet, then select either **Allow** or **Deny** from the drop list.
In our example, the HTTP service is set to Allow enabling Web traffic incoming.
- 3 Enter the trusted network IP address of the computer to which this rule applies.
In our example, 192.168.111.2.
- 4 Click **Submit**.

Create a Custom Service

In addition to the pre-configured services provided by the SOHO 6 configuration page, you can create custom services using either a TCP port, UDP port or specifying an IP protocol.

Follow these steps to create a custom service:

- 1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: <http://192.168.111.1>

- From the navigation bar on the left side, select **Firewall** ⇒ **Custom Service**.

The Custom Service page appears.

The screenshot shows the 'Custom Service' configuration page. On the left is a navigation sidebar with categories: System Status, Network, Administration, Firewall, Logging, and WebBlocker. The 'Firewall' section is expanded, and 'Custom Service' is selected. The main content area is titled 'Firewall Custom Service'. It contains several fields: 'Service Name' (text input), 'Protocol Settings' (a table with 'Protocol' and 'Port' columns, a 'Remove' button, and a 'TCP Port' dropdown with 'Add' and 'To' fields), 'Incoming Filter' (dropdown set to 'No Rule'), 'Service Host' (text input set to '0.0.0.0'), 'From' (text input set to 'Any' with a 'Remove' button), 'Host IP Address' (dropdown set to '0.0.0.0' with an 'Add' button), and 'Outgoing Filter' (dropdown set to 'No Rule').

- Define a name for the service in the appropriate field.
- Beneath the Protocol Settings fields, select either **TCP Port**, **UDP Port**, or **Protocol** from the drop list.

The Custom Service page refreshes.

NOTE

In addition to TCP and UDP ports, there are several other types of Internet protocols. To create a service for one of these protocols, you must define the protocol number—you cannot specify a port number.

- 5 Enter the port number (or numbers if creating a range of ports) or enter the IP protocol number to allow in the appropriate fields and click **Add**.

After creating a custom service, you need to specify a filter rule as well as define the incoming and outgoing properties.

- 6 At the Incoming and Outgoing Filter drop lists, select either **Allow** or **Deny**.
- 7 Select either Host IP Address, Network IP Address, or Host Range from the appropriate drop list.
The Custom Service page refreshes.
- 8 Enter either a single host IP address, a network IP address, or the start and end of a range of host IP addresses for this custom service in the appropriate fields.
- 9 Click **Add**.
Repeat the last three steps until all the appropriate address information for this custom service appears in the appropriate fields.
- 10 Click **Submit**.

Block External Sites

By default, the security stance of the SOHO 6 is to deny all incoming traffic to the trusted network, but to allow all outgoing traffic. However, you can selectively block access to particular Internet sites entirely.

Follow these steps to configure blocked sites:

- 1 From the navigation bar on the left side, select **Firewall** ⇒ **Blocked Sites**.

The Blocked Sites page appears.

The screenshot shows the 'Blocked Sites' configuration page. On the left is a navigation menu with categories: System Status, Network, Administration, Firewall, and Blocked Sites. The main content area is titled 'Firewall Blocked Sites'. It features a large empty rectangular field labeled 'Blocked Sites'. To the right of this field is a 'Remove' button. Below the field is a form with a dropdown menu labeled 'Host IP Address' (currently showing 'Host IP Address'), a text input field containing '0.0.0.0', and an 'Add' button. At the bottom of the page are 'Submit' and 'Reset' buttons.

- 2 Select either Host IP Address, Network IP Address, or Host Range from the drop list.
The Blocked Sites page refreshes.
- 3 Enter either a single host IP address, a network IP address, or the start and end of a range of host IP addresses in the appropriate fields.
In our example, Host IP Address is selected and the IP address entered is 207.68.172.246.
- 4 Click **Add**.
The addressing appears in the Blocked Sites field.
- 5 Click **Submit**.

Firewall Options

The SOHO 6 firewall feature includes a few rule settings that are less specific than the service settings discussed previously and are used to provide further security for your private network. These options are found on the Firewall Options page.

- 1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: <http://192.168.111.1>
- 2 From the navigation bar on the left side, select **Firewall** ⇒ **Firewall Options**.
The Firewall Options page appears.

System Status Network External Trusted Optional Routes Network Statistics DynamicDNS Administration System Security VPN Manager Access Update Upgrade View Configuration File Firewall Incoming Outgoing Custom Service Blocked Sites Firewall Options	Firewall Firewall Options <hr/> <input type="checkbox"/> Do not respond to PING requests received on External Network. <input type="checkbox"/> Do not allow FTP access to Trusted Network interface. <input type="checkbox"/> Disable SOCKS proxy. <input type="checkbox"/> Log All Allowed Outbound Access. <hr/> <input type="checkbox"/> Enable override MAC address for the External Network. External Network override MAC address <input style="width: 100px;" type="text"/> <hr/> <input type="button" value="Submit"/> <input type="button" value="Reset"/>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Ping requests received on the External Network

You can configure the SOHO 6 to deny all ping packets that it receives on the external interface.

- 1 Select **Do not respond to PING requests received on External Network**.
- 2 Click **Submit**.

Denying FTP access to the Trusted Network interface

You can configure the SOHO 6 to deny FTP access to the Trusted interface.

- 1 Select **Do not allow FTP access to Trusted Network**.
- 2 Click **Submit**.

SOCKS implementation for the SOHO 6

SOCKS is a network proxy filter that works with SOCKS-aware applications. A typical SOCKS-dependent application requires that several sockets be opened and made available to the Internet.

When a SOCKS-aware application (ICQ is an example) registers with the SOCKS server, SOCKS is able to manage the need of the application to have many ports open.

To use an application with SOCKS, configure the application with the SOCKS server information.

Setting up your SOCKS application for use with the SOHO 6 requires no reconfiguration of the SOHO 6 appliance itself. Your SOHO 6 acts as the SOCKS proxy. You must, however, configure your application to be compliant with the SOHO 6 implementation of SOCKS version 5.

The SOHO 6 SOCKS feature has the following characteristics and limitations:

- SOHO 6 supports SOCKS version 5 only.
- It is a limited version of SOCKS and does not support authentication.

NOTE

Configure the particular application so that it does *not* attempt to make DNS look-ups with SOCKS. Some applications use only DNS through SOCKS and therefore do not function properly with the SOHO 6.

- Compatible SOCKS-aware applications that are used through the SOHO 6 include ICQ, IRC, and AOL Messenger.
- When you open a SOCKS application, it opens a “hole” in the SOHO 6 firewall making the computer running the application available to anyone on your trusted network. SOCKS applications therefore pose a significant security risk. To disable the port and close the security risk, see “Disabling SOCKS on the SOHO 6” on page 70.

Configuring your SOCKS application

Other than making certain that port 1080 is open to run a SOCKS-dependent application, the rest of the configuration tasks is done with the SOCKS-dependent application. Different applications may have variations in their settings, but you configure the SOCKS-dependent application, using the application user interface, to certain parameters allowing the SOHO 6 to pass SOCKS applications:

- If different services or versions of SOCKS are available, select SOCKS version 5.
- Select port 1080 for the application

- For the SOCKS proxy, enter the URL or IP address of the SOHO 6 trusted network. The default IP address is 192.168.111.1.

Disabling SOCKS on the SOHO 6

Once you use a SOCKS-compliant application through the SOHO 6, the primary SOCKS port is available to anyone on your trusted network. You can close this security gap between uses of SOCKS applications.

- 1 Enable the checkbox labeled **Disable SOCKS proxy**.
This disables the SOHO 6 from acting as a SOCKS proxy.
- 2 Click **Submit**.

When you need to use SOCKS again, follow this procedure:

- 1 Disable the checkbox labeled **Disable SOCKS proxy**.
This enables the SOHO 6 to act as a SOCKS proxy.
- 2 Click **Submit**.
The SOHO 6 is enabled again as a Proxy server and ready to pass SOCKS packets.

Logging all allowed outbound traffic

By default, the SOHO 6 logs only particular events and *not* all traffic passing through it. For the most part, the SOHO 6 records denied traffic. However, the SOHO 6 is able to record all allowed outbound traffic.

NOTE

This option will record an extensive amount of log entries. For this reason, WatchGuard recommends that you use it for diagnostic purposes only.

Follow these steps:

- 1 Select **Log All Allowed Outbound Access**.
- 2 Click **Submit**.

Enable override MAC address for the External Network

A SOHO administrator is able to assign a second MAC address to the SOHO 6 External Network making it easier to register with an ISP that requires a separate MAC for registration.

- 1 Select **Enable override MAC address for the External Network**.
- 2 Enter the MAC address that will be assigned to the SOHO 6 External Network.

NOTE

If the External Network override MAC address text box is cleared and the SOHO 6 is rebooted, the SOHO 6 will automatically go back to the factory-default External MAC address.

- 3 Click **Submit**.

As a guard against MAC address collisions, the SOHO 6 will look for the External Network override MAC address periodically. If the SOHO 6 finds two devices on the local network with the same MAC address, the SOHO 6 will automatically reset itself to the factory-default External MAC address and reboot.

Create an Unrestricted Pass Through

The SOHO 6 is able to allow traffic to be passed through to a dedicated machine with a public IP address separated from the rest of the Trusted network.

Follow these steps to configure a pass through:

- 1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: `http://192.168.111.1`
- 2 From the navigation bar on the left side, select **Firewall** ⇒ **Pass Through**.
The Unrestricted Pass Through IP Address page appears.

The screenshot shows the web interface for configuring the Unrestricted Pass Through IP Address. On the left is a navigation menu with categories: System Status, Network, and Administration. Under Network, 'Firewall' is selected, and 'Unrestricted Pass Through IP Address' is the active page. The main content area has a heading 'Unrestricted Pass Through IP Address' and a checkbox labeled 'Enable pass through address' which is checked. Below this is a text input field labeled 'Address to pass through' containing the IP address '208.253.208.103'. At the bottom are 'Submit' and 'Reset' buttons.

- 3 Select **Enable pass through address**.
- 4 Enter the IP address to the pass through machine in the appropriate field. This *must* be a public IP address.
In our example, 208.253.208.103.
- 5 Click **Submit**.

NOTE

Use of the Pass Through feature increases the security risk to computers on the Trusted network. This is because the computer using the Pass Through resides on the same Ethernet segment as the Trusted network. If you are not completely and thoroughly familiar with the risks involved

and Trusted network computers are not protected from potential threats, do not use the Pass Through feature

Configure Logging

What is logging? Logging is the act of recording “events” that occur at the SOHO 6 interfaces. An event is any single activity, such as communication with the WatchGuard WebBlocker database or incoming traffic passing through the SOHO 6.

Logging is intended to record the kinds of activities that indicate security concerns—most importantly denied packets. Certain patterns of denied packets can indicate the type of attack that is being attempted. Remember that if power to the SOHO 6 is removed the messages are lost.

View SOHO 6 Log Messages

The WatchGuard SOHO 6 generates an ongoing activity log stored on the SOHO 6: the Event Log. This log stores a maximum of 150 messages. When it reaches this limit, the oldest message is deleted.

The log messages include time synchronizations between the SOHO 6 and the WatchGuard Time Server, discarded packets for a packet handling violation, duplicate messages, or return error messages and IPSec messages.

To view these messages:

- 1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: <http://192.168.111.1>.
- 2 From the navigation bar on the left side, select **Logging**.
The Logging page appears and the Event Log is displayed in the lower portion of the page.

The screenshot shows the 'Logging' configuration page. On the left is a navigation sidebar with categories: System Status, Network (External, Trusted, Optional, Routes, Network Statistics, DynamicDNS), Administration (System Security, VPN Manager Access, Update, Upgrade, View Configuration File), and Firewall (Incoming). The main content area has a 'Logging' header. Below it is a 'Logging Options' section with two rows: 'WSEF Logging' (Disabled, WSEF Log Host 0.0.0.0, Configure) and 'Syslog Logging' (Disabled, Syslog Host 0.0.0.0, Configure). Below that is a 'System Time' section (Configure) with fields for Time Zone, DST (Disabled), Time Source (WatchGuard Time Server), and Current Time (2002-11-23-00:27:15). At the bottom is a 'Sync Time With Browser Now' button.

NOTE

The SOHO 6 displays the latest entry at the top of the Event Log.

To have your log messages synchronize with your computer:

- Click **Sync Time with Browser now**.

The SOHO 6 synchronizes the time at startup.

Set up Logging to a WatchGuard Security Event Processor Log Host

The WSEP (WatchGuard Security Event Processor) is an application available with the WatchGuard Firebox System software used by a Firebox II/III. The WSEP application runs on a dedicated log host and records log messages generated by the Firebox II/III. If you have a Firebox II/III and have configured the WSEP to accept logs from your SOHO 6, then follow these instructions to send your event logs to the WSEP.

- 1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: <http://192.168.111.1>.
- 2 From the navigation bar on the left side, select **Logging ⇒ WSEP Logging**.

The WatchGuard Security Event Processor page appears.

System Status
Network
External
Trusted
Optional
Routes
Network Statistics
DynamicDNS
Administration
System Security
VPN Manager Access
Update
Upgrade
View Configuration File

Logging
WatchGuard Security Event Processor Logging

Enable WatchGuard Security Event Processor Logging

Log Host IP Address

Log Encryption Key

Confirm Key

- 3 Select **Enable WatchGuard Security Event Processor Logging**.
- 4 Enter the IP address of the WSEP server that is your log host in the appropriate field.
In our example, 192.168.111.5.
- 5 In the **Log Encryption Key** field, enter a passphrase and confirm it.
- 6 Click **Submit**.

NOTE

This encryption key must be identical to the one used in the WSEP.

Set up Logging to a Syslog Host

The SOHO 6 also sends log entries to a Syslog host.

Follow these steps to setup a Syslog Host:

- 1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: `http://192.168.111.1`.
- 2 From the navigation bar on the left side, select **Logging** ⇒ **Syslog Logging**.
The Syslog Logging page appears.

The screenshot shows the configuration page for Syslog Logging. On the left is a navigation menu with the following items: System Status, Network (External, Trusted, Optional, Routes, Network Statistics, DynamicDNS), and Administration (System Security, VPN Manager Access). The main content area is titled "Logging" and "Syslog Logging". It features a checkbox for "Enable syslog output", a text input field for "Address of syslog host" containing "0.0.0.0", and another checkbox for "Include local time in syslog message". At the bottom of the form are "Submit" and "Reset" buttons.

- 3 Select **Enable syslog output**.
- 4 Enter the IP address of the Syslog server.
In our example, 206.253.208.100.
- 5 Click **Submit**.

To adjust your syslog messages to your browsers local time:

- Select **Include local time in syslog message**.

NOTE

Syslog traffic is not encrypted and use of this option creates a potential security risk when the information is sent over the Internet. However, if this traffic is sent through a VPN tunnel the traffic is encrypted with IPSec technology and therefore less of a security risk.

Set the System Time

The SOHO 6 stamps each log entry with the time that the event occurred.

Event Log		
Time	Category	Message
2002-05-23-17:16:09	IP	Packet allowed from 192.168.42.204 port 3577 to 192.168.42.160 port 80 (TCP)(allow by HTTP)
2002-05-23-17:16:08	MONITOR	Administrator access allowed from 192.168.42.204
2002-05-23-17:16:08	IP	Packet allowed from 192.168.42.204 port 3576 to 192.168.42.160 port 80 (TCP)(allow by HTTP)

The log entry time stamp displays the time of day according to the settings for the system time.

To set the system time:

- 1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: <http://192.168.111.1>.
- 2 From the navigation bar on the left side, select **Logging ⇒ System Time**.

The System Time page appears.

The screenshot shows the 'System Time' configuration page. On the left is a navigation sidebar with categories: System Status, Network (External, Trusted, Optional, Routes, Network Statistics, DynamicDNS), Administration (System Security, VPN Manager Access, Update, Upgrade, View Configuration File), and Firewall (Incoming, Outgoing, Custom Service). The main content area has a breadcrumb trail: Logging > System Time. Below this is the 'Time Source' section with two radio button options: 'Get Time From TCP Port 37 Time Server at' (with an empty text input field) and 'Get Time From WatchGuard Time Server' (which is selected). The 'Time Zone' section includes a note: 'Time Zone adjustments are only applied when using the WatchGuard time server'. Below the note is a dropdown menu currently showing '(GMT-12:00) Eniwetok, Kwajalein'. There is also an unchecked checkbox for 'Adjust for daylight savings time'. At the bottom of the form are 'Submit' and 'Reset' buttons.

If you have decided to use the WatchGuard Time Server:

3 Select **Get Time From WatchGuard Time Server**.

Or, to use a TCP Port 37 Time Server:

4 Select **Get Time From TCP Port 37 Time Server at**.

5 Enter the IP address of the time server in the appropriate field.

6 Click **Submit**.

To adjust your log messages for daylight savings time or set the time zone:

- Select **Adjust for daylight savings time**.
- Select a time zone from the drop list.

Time Zone adjustments are only applied when using the WatchGuard time server.

VPN—Virtual Private Networking

This chapter describes an optional feature of the WatchGuard SOHO 6, Virtual Private Networking (VPN) with IPSec.

Why Create a Virtual Private Network?

Virtual Private Networking (VPN) tunnels enable you to securely connect computers in two locations without requiring expensive, dedicated point-to-point data connections. With VPN, you use low cost connections to the Internet to create a virtual connection between two branch offices. Unlike a simple, unencrypted Internet connection, a VPN connection eliminates any significant risk of data being read or altered by outside users as it traverses the Internet.

What You Need

- One WatchGuard SOHO 6 with VPN and an IPSec-compliant appliance.

NOTE

While you can create a SOHO 6 to SOHO 6 VPN, you can also create a VPN with a WatchGuard Firebox II/III, Firebox Vclass, or other IPSec-compliant appliances.

- The following information from your Internet service provider for both appliances:
 - Static IP address
 - Primary DNS (Domain Name Service) IP address (optional)
 - If available, a secondary DNS address
 - Domain name (optional)
- Network addresses and subnet mask for networks. By default, the Trusted network address of the SOHO 6 is 192.168.111.0 and the subnet mask is 255.255.255.0.

NOTE

The internal networks on either end of the VPN tunnel must use different network addresses.

To create an IPSec tunnel between appliances you must add information to the configuration files of each that is specific to the site, such as external and trusted IP addresses. It is imperative to keep these addresses accurate. WatchGuard recommends making a table of IP addresses such as the one outlined below.

IP Address Table (example):

Item	Description	Assigned By
External IP Address	<p>The IP address that identifies the SOHO 6 to the Internet.</p> <p>Site A: 207.168.55.2 Site B: 68.130.44.15</p>	ISP
External Subnet Mask	<p>The overlay of bits that determines which part of the IP address identifies your network. For example, a Class C address licenses 256 addresses and has a netmask of 255.255.255.0.</p> <p>Site A: 255.255.255.0 Site B: 255.255.255.0</p>	ISP
Local Network Address	<p>A private network address used by an organization's local network for identifying itself within the network. A local network address cannot be used as an external IP address. WatchGuard recommends using an address from one of the reserved ranges:</p> <p>10.0.0.0/8 172.16.0.0/12—255.240.0.0 192.168.0.0/16—255.255.0.0</p> <p>Site A: 192.168.111.0/24 Site B: 192.168.222.0/24</p>	You
Shared Secret	<p>A phrase stored at both ends of the tunnel to authenticate the transmission as being from the claimed origin. The secret can be any phrase, but mixing numerical, special, alphabetical, and uppercase characters improves security. For example, "Gu4c4mo!3" is better than "guacamole"</p> <p>Site A: OurLittleSecret Site B: OurLittleSecret</p>	You
Encryption Method	<p>Encryption method determines the length in bits of the key used to encrypt and decrypt communication packets. DES is a 56-bit encryption; 3DES is 168-bit, and much more secure. It is also slower. Select either 3DES or DES as long as both sides use the same method.</p> <p>Site A: 3DES Site B: 3DES</p>	You

Authenticati on	Both sides must use the same method.	You
	Site A: MD5 (or SHA1)	
	Site B: MD5 (or SHA1)	

Enable the VPN Upgrade

You must first redeem the VPN upgrade license key before configuring VPN. Activating the VPN upgrade requires:

- An installed SOHO 6
- Internet connectivity
- A VPN upgrade license key

Step-by-step Instructions for Configuring a SOHO 6 VPN Tunnel

WatchGuard has developed a series of step-by-step instructions to facilitate configuration for a SOHO 6 VPN tunnel to any of several other IPSec-compliant appliances. To download these instructions using your Web browser, go to:

https://support.watchguard.com/AdvancedFaqs/sointerop_main.asp

Special Considerations

Consider the following before configuring your WatchGuard SOHO 6 VPN network:

- You can connect up to six SOHO 6 appliances together. To set up more VPN tunnels, you need at least one WatchGuard Firebox II/III configured with the WatchGuard VPN Manager.
- Each appliance must be able to send messages to the other. If either appliance has a dynamically assigned IP address (see “Network addressing” on page 31 for an explanation of dynamic IP addresses), that appliance cannot find its remote counterpart.
- Both appliances must use the same encryption method. The two choices are DES or 3DES. When connecting two Microsoft Windows NT[®] networks, the two networks must be in the same Microsoft Windows domain or be trusted domains. This is a Microsoft Networking design implementation and not a limitation of the SOHO 6.

Frequently Asked Questions

Why do I need a static external address?

To create a VPN connection, one SOHO 6 must be able to find its partner appliance. If the addresses are allowed to change, the SOHO 6 will not find its remote computer.

How do I get a static external IP address?

Contact your ISP. Many systems use dynamically assigned addresses to simplify basic installations. Some providers also use

this feature to discourage users from creating Web servers. These providers usually offer a static IP address option.

How do I troubleshoot the connection?

If you are able to ping the remote SOHO 6 and computers behind it, your VPN tunnel is up and running. Any remaining problems are probably caused by the MS Networking or the applications being used.

Why is ping not working?

If you cannot ping the local network address of the remote SOHO 6, follow these steps to classify the problem:

- 1 Ping the external address of the remote SOHO 6.
For example, at Site A, ping 68.130.44.15 (Site B). You should get a reply. If not, verify the External network settings of Site B. If they are correct, verify that computers at Site B have access to the internet. If you are still having trouble, contact your ISP.
- 2 Once you are able to ping the external address of each SOHO 6, try pinging a local address.
From Site A, ping 192.168.111.1. If the tunnel is up, you should get a reply from the remote SOHO 6. If not, re-check the local settings page. Make sure that the local DHCP address ranges do not overlap. That is, IP addresses on either side of the tunnel *must not* be the same.

How do I obtain a VPN upgrade license key?

You can purchase them online. Using your Web browser, go to:

<http://www.watchguard.com/sales/buyonline.asp>

How do I enable a VPN Tunnel?

Full instructions for enabling a VPN tunnel are located at:

https://support.watchguard.com/AdvancedFaqs/sointerop_main.asp

Set Up Multiple SOHO-SOHO VPN Tunnels

With this release, a SOHO administrator has the ability to manually define up to six VPN tunnels to other SOHO 6 devices. VPN Manager's ability to set up a larger number of SOHO 6 to SOHO 6 tunnels remains.

To define multiple VPN tunnels to other SOHO 6 appliances:

- 1 With your Web browser, go to the System Status page using the trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: `http://192.168.111.1`
- 2 From the navigation bar on the left side, select **VPN ⇒ Manual VPN**.
The Manual VPN page appears.
- 3 Click **Add**.

The Add Gateway page appears.

System Status

Network

- External
- Trusted
- Optional
- Routes
- Dual ISP
- Network Statistics
- DynamicDNS

Administration

- System Security
- VPN Manager Access
- Update
- Upgrade
- View Configuration File

Firewall

- Incoming
- Outgoing
- Custom Service
- Blocked Sites
- Firewall Options
- Pass Through

Logging

- WSEP Logging
- Syslog Logging
- System Time

WebBlocker

VPN

- Managed VPN
- Manual VPN
- MUVPN Clients
- VPN Statistics

VPN > Manual VPN

Add Gateway

Name

Shared Key

Phase 1 Settings

Because your external IP address is not fixed, you must use Aggressive Mode and the Local ID type must be Domain Name.

Local ID Type

Remote ID Type

Authentication Algorithm

Encryption Algorithm

Negotiation expiration in kilobytes

Negotiation expiration in hours

Diffie-Helman Group

Enable Perfect Forward Secrecy

Generate IKE Keep Alive Messages

Phase 2 Settings

Authentication Algorithm

Encryption Algorithm

Key expiration in kilobytes

Key expiration in hours

Local Network	Remote Network
<input type="text"/>	<input type="text"/>

- 4 Enter the **Name**, **IPSec Gateway Address**, and **Shared Key** for SOHO 6 you want to set up a VPN tunnel.

The shared key is used by the local and remote SOHO to encrypt and decrypt the data going across the tunnel. The shared key is the same on both ends of the tunnel. The gateways can encrypt and decrypt the data correctly only if they share the same key.

- 5 Phase 1 setting can be left at the defaults shown or modified as desired. To modify Phase 1 settings, complete the following

- steps. Make sure that the Phase 1 settings on this device are the same as on the peer device.
- 6 Select the type of negotiation for Phase 1. The two Mode Types are Main and Aggressive. If your external IP address is dynamic, you must use Aggressive Mode, otherwise you may use either option.
 - 7 Enter the local and remote ID types. These must match the settings used on the remote gateway.
 - If you are using Main Mode, the Local and Remote ID Type must be an IP Address.
 - If you are using Aggressive Mode, the Remote ID Type may be either IP Address or Domain Name. If your external IP address is fixed, the Local ID Type must be IP address, otherwise your Local ID Type may be either Domain Name or IP Address.
 - 8 In the **Local ID** and **Remote ID** box, specify the name of the local or remote network. The default is LocalID and RemoteID. In the **Type** box, specify IP Address or Domain Name.

If you are in Main Mode, both the Local and Remote IDs must be IP Address. If you are in Aggressive Mode and have a static IP address, the Local ID must be IP Address and the Remote ID can be either IP Address or Domain Name. If you are in Aggressive Mode and have a dynamic IP address, the Local ID must be Domain Name and the Remote ID can be either IP Address or Domain Name.
 - 9 In the **Authentication Algorithm** drop list, specify the authentication: MD5-HMAC (128-bit authentication) or SHA1-HMCA (160-bit authentication).
 - 10 In the **Encryption Algorithm** drop list, specify the type of encryption: DES-CBC or 3DES-CBC.
 - 11 Enter how many kilobytes until negotiation expiration.
 - 12 Enter how many hours until negotiation expiration.

- 13 In the **Diffie-Hellman Group** drop list, specify the group. WatchGuard supports 1 & 2.
Diffie-Hellman refers to a mathematical technique for securely negotiating secret keys over a public medium. Diffie-Hellman groups are collections of parameters used to achieve this. Group 2 is more secure than group 1, but requires more time to compute the keys.
- 14 If you choose, select the checkbox marked **Enable Perfect Forward Secrecy**.
When this option is selected, each new key that is negotiated is derived by a new Diffie-Hellman exchange instead of from only one Diffie-Hellman exchange. Enabling this option provides more security, but requires more time because of the additional exchange.
- 15 Enable the **Generate IKE Keep Alive Messages** checkbox to keep a VPN tunnel from going down because of time out conditions. A small amount of traffic is sent across the VPN tunnel to keep it alive and functioning. If the tunnel fails for any reason the SOHO 6 initiates a rekey of the tunnel to restore it.
This checkbox is enabled by default.
- 16 Phase 2 setting can be left at the defaults shown or modified as desired. To modify Phase 2 settings, complete the following steps. Make sure that the Phase 2 settings on this device are the same as on the peer device.
- 17 In the **Authentication Algorithm** drop list, specify the authentication: None (no authentication), MD5-HMAC (128-bit authentication) or SHA1-HMCA (160-bit authentication).
- 18 In the **Encryption Algorithm** drop list, specify the type of encryption: None (no authentication), DES-CBC or 3DES-CBC.
- 19 Enter how many kilobytes until key expiration.
- 20 Enter how many hour until key expiration.
- 21 Add the IP address of the local and remote network that will use Phase 2 negotiation.
- 22 Click **Submit**.

Configure Split Tunneling

Another new feature in this release is split tunneling that allows the administrator to specify all Internet traffic originating from the Trusted interface of the SOHO 6 to go through the VPN tunnel. Previously, only traffic headed specifically for the other end of the VPN tunnel was sent through the tunnel; Traffic destined for other Internet addresses was sent directly to the Internet. Split tunneling allows a company to centrally enforce an Internet access policy.

To set up split tunneling:

- 1 With your Web browser, go to the System Status page using the trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: <http://192.168.111.1>
- 2 From the navigation bar on the left side, select **VPN ⇒ Manual VPN**.
The Manual VPN page appears.
- 3 Click **Add**.
The Add Gateway page appears.
- 4 Enter the information to add the gateway.
For instructions on completing the Add Gateway page, see "Set Up Multiple SOHO-SOHO VPN Tunnels" on page 89.
- 5 Type the network IP address of the **Local Network**.
- 6 Type 0.0.0.0/0 as the IP address of the **Remote Network**.
- 7 Click **Submit**.

MUVPN Clients

The SOHO 6 can be upgraded to use the MUVPN clients option. This feature allows remote users to securely connect to the SOHO 6 through an IPSec VPN tunnel. The remote user gains access to the local trusted network and networks on Branch Office VPN tunnels

terminating at the local SOHO 6. The SOHO 6 also allows users on the Trusted network to access networks on Branch Office VPN tunnels terminating at the local SOHO 6. If you purchase the VPNforce Port, you receive one MUVPN connection to the Optional network as well. Additional VPNforce Port user licenses can be purchase separately. Complete documentation on configuring your SOHO 6 once this upgrade option is purchased and redeemed are at:

<http://support.watchguard.com/sohoresources/>

View the VPN Statistics

The SOHO 6 has a configuration page that displays a variety of VPN statistics to assist you in monitoring VPN traffic as well as troubleshooting potential problems.

To view the VPN Statistics page:

- 1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: <http://192.168.111.1>.
- 2 From the navigation bar on the left side, select **VPN ⇒ VPN Statistics**.
The VPN Statistics page appears.

WebBlocker is an optional feature of the SOHO 6 that provides Web site filtering capabilities. It gives you precise control over the types of Web sites users on your trusted network are allowed to view.

How WebBlocker Works

WebBlocker relies on a URL database service, which is owned and maintained by SurfControl. The WebBlocker database contains many thousands of IP addresses and directories. These addresses are divided into categories based upon content such as drug culture, intolerance, or sexual acts.

WatchGuard updates the Webblocker server with a new database at regular intervals.

Once you purchase and activate WebBlocker, every time a user on your trusted network attempts to reach an Internet Web site, the

SOHO 6 queries the WatchGuard database and determines whether or not to block the site. The SOHO 6 considers the following conditions in determining whether or not to block the site:

Web site not in the WebBlocker database

If the site is not in the WatchGuard WebBlocker database, the Web browser opens the page for viewing.

Web site in the WebBlocker database

If the site is in the WatchGuard WebBlocker database, the SOHO 6 checks whether or not to block that type (or category) of site. When the category is blocked, the browser displays a page informing the user that the site is unavailable for viewing. If the category is not blocked, the Web browser opens the page for viewing.

WatchGuard WebBlocker database unavailable

If for any reason the WatchGuard WebBlocker database is unavailable (for example, if there is briefly a problem between your ISP and the nearest WatchGuard server), the browser displays a page informing the user that the site is unavailable for viewing.

WebBlocker users and groups

Groups

A group is a collection of individuals or users of the system.

Users

These are individual members of a particular group.

Bypass the SOHO 6 WebBlocker

Occasionally, you may want to allow select individuals to bypass the filtering functions of SOHO 6 WebBlocker. For example, if you are using the SOHO 6 at a remote office as a telecommuter, you may want to block a particular category from your children while still retaining access to that information for the adults in the household.

The SOHO 6 WebBlocker configuration page includes a full access password field. Provide this password to those members of your trusted network allowed to bypass WebBlocker. When a site is blocked or unavailable, the user has the option of entering the full access password. With the password entered, the browser displays the otherwise blocked site. After the password is entered, the user is able to browse any site on the Internet until either the password expires or the browser is closed.

Purchase and Activate SOHO 6 WebBlocker

To use WatchGuard SOHO 6 WebBlocker, you must first purchase and enable the WebBlocker upgrade license key. For information on redeeming upgrade license keys, see, “Redeem your SOHO 6 Upgrade Options” on page 57.

Configure the SOHO 6 WebBlocker

Use the WatchGuard SOHO 6 Configuration pages to activate WebBlocker, create a full access password for bypassing WebBlocker, define an inactivity timeout that sets the duration of the full access password, define the categories you want to block, and configure WebBlocker groups and users.

Activate WebBlocker

Follow these instructions to activate WebBlocker, create a full access password, define the inactivity timeout value, and require that your Web users authenticate (if your are using the groups and users feature option).

- 1 With your Web browser, go to the SOHO 6 Configuration Settings page using the Trusted IP address of the SOHO 6. For example, if using the default IP address, go to: `http://192.168.111.1`
- 2 From the navigation bar on the left side, select **WebBlocker => Settings**.
The WebBlocker Settings page appears.

The screenshot shows the configuration interface for WebBlocker. On the left is a navigation menu with categories: System Status, Network (External, Trusted, Routes, Network Statistics, DynamicDNS), Administration (System Security, VPN Manager Access, Update, Upgrade, View Configuration File), and Firewall (Incoming). The main content area is titled 'WebBlocker Settings' and contains the following options:

- Enable WebBlocker
- Full Access Password:
- Confirm Password:
- Inactivity Timeout (minutes):
- Require Web users to authenticate

At the bottom of the settings area is a **Submit** button.

- 3 Select **Enable WebBlocking**.
- 4 Enter the full access password.
The full access password allows a user a to bypasses otherwise blocked sites.
- 5 Enter the inactivity timeout in minutes.
For example, setting the inactivity timeout at 15 minutes ensures that unattended Web browsers are disconnected after sitting idle for 15 minutes.
- 6 If you intend to use WebBlocker groups and users, select **Require Web users to authenticate**.
- 7 Click **Submit** to register your changes.

Create WebBlocker Groups and Users

Follow these instructions to create WebBlocker Groups.

- 1 With your Web browser, go to the SOHO 6 Configuration Settings page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: <http://192.168.111.1>
- 2 From the navigation bar on the left side, select **WebBlocker ⇒ Groups**.

The WebBlocker Groups page appears.

System Status

Network

- External
- Trusted
- Routes
- Network Statistics
- DynamicDNS

Administration

- System Security
- VPN Manager Access
- Update
- Upgrade
- View Configuration File

Firewall

- Incoming
- Outgoing
- Custom Service
- Blocked Sites
- Firewall Options
- Pass Through
- Logging

WebBlocker Groups

Group [Default Group](#)

Users [All Users](#)

Blocked Categories

<input type="checkbox"/> Alcohol and Tobacco	<input type="checkbox"/> Violence/Profanity
<input type="checkbox"/> Illegal Gambling	<input type="checkbox"/> Search Engines
<input type="checkbox"/> Militant/Extremist	<input type="checkbox"/> Sports and Leisure
<input type="checkbox"/> Drug Culture	<input type="checkbox"/> Sex Education
<input type="checkbox"/> Satanic/Cult	<input type="checkbox"/> Sex Acts
<input type="checkbox"/> Intolerance	<input type="checkbox"/> Full Nudity
<input type="checkbox"/> Gross Depictions	<input type="checkbox"/> Partial/Artistic Nudity

- 3 Click **New** to create a group name and profile.

The screenshot shows the configuration page for creating a new group in the SOHO 6 WebBlocker. On the left is a navigation menu with categories: System Status, Network, Administration, and Firewall. The main content area is titled 'WebBlocker > Groups' and 'New Group'. It features a 'Group Name' text box containing 'chicosmalos'. Below this is a 'Blocked Categories' section with a grid of checkboxes. At the bottom are 'Submit', 'Reset', and 'Cancel' buttons.

Category	Selected
Alcohol and Tobacco	<input type="checkbox"/>
Violence/Profanity	<input checked="" type="checkbox"/>
Illegal Gambling	<input type="checkbox"/>
Search Engines	<input type="checkbox"/>
Militant/Extremist	<input checked="" type="checkbox"/>
Sports and Leisure	<input type="checkbox"/>
Drug Culture	<input checked="" type="checkbox"/>
Sex Education	<input type="checkbox"/>
Satanic/Cult	<input type="checkbox"/>
Sex Acts	<input checked="" type="checkbox"/>
Intolerance	<input type="checkbox"/>
Full Nudity	<input checked="" type="checkbox"/>
Gross Depictions	<input checked="" type="checkbox"/>
Partial/Artistic Nudity	<input type="checkbox"/>

4 Define a Group Name and select the blocked categories for this group.

5 Click **Submit**.

A new Groups page appears indicating the configuration changes were accepted and are providing access.

WebBlocker
Groups

Configuration changes have been accepted.

Group

Users

- 6 To the right of the Users field, click **New**.
The New User page appears.

WebBlocker > Groups
New User

User name

Passphrase

Confirm Passphrase

Group

- 7 Enter a unique user name and passphrase (remember to confirm the passphrase). Use the Group drop list to assign the new user to a given group.

8 Click **Submit**.

NOTE

You can delete users or groups at any time by selecting them and clicking **Delete**.

WebBlocker Categories

WebBlocker relies on a URL database, which is a service of SurfControl. The WebBlocker database contains thousands of IP addresses and directories. These addresses are divided into categories based on content such as drug culture, intolerance, or sexual acts. SurfControl constantly searches the Internet to update the list of blocked sites. The WebBlocker database contains the following 14 categories.

NOTE

All the categories of sites to be blocked are selected by advocacy rather than opinion or educational material. For example, the drugs/drug culture category blocks sites describing how to grow and use marijuana but does not block sites discussing the historical use of marijuana.

Alcohol/tobacco

Pictures or text advocating the sale, consumption, or production of alcoholic beverages and tobacco products.

Illegal Gambling

Pictures or text advocating materials or activities of a dubious nature that may be illegal in any or all jurisdictions, such as illegal business schemes, chain letters, copyright infringement, computer hacking, phreaking

(using someone's phone lines without permission), and software piracy. Also includes text advocating gambling relating to lotteries, casinos, betting, numbers games, online sports, or financial betting, including non-monetary dares.

Militant/extremist

Pictures or text advocating extremely aggressive or combative behavior or advocacy of unlawful political measures. Topic includes groups that advocate violence as a means to achieve their goals. It also includes pages devoted to "how to" information on the making of weapons (for both lawful and unlawful reasons), ammunition, and pyrotechnics.

Drug Culture

Pictures or text advocating the illegal use of drugs for entertainment. This category includes substances that are used for other than their primary purpose to alter the individual's state of mind, such as glue sniffing. This does not include (that is, if selected these sites would not be WebBlocked under this category) currently illegal drugs legally prescribed for medicinal purposes (such as, drugs used to treat glaucoma or cancer).

Satanic/cult

Pictures or text advocating devil worship, an affinity for evil, wickedness, or the advocacy to join a cult. A cult is defined as: a closed society that is headed by a single individual where loyalty is demanded and leaving is punishable.

Intolerance

Pictures or text advocating prejudice or discrimination against any race, color, national origin, religion, disability

or handicap, gender, or sexual orientation. Any picture or text that elevates one group over another. Also includes intolerant jokes or slurs.

Gross Depictions

Pictures or text describing anyone or anything that is either crudely vulgar, grossly deficient in civility or behavior, or shows scatological impropriety. Topic includes depictions of maiming, bloody figures, and indecent depiction of bodily functions.

Violence/profanity

Pictures or text exposing extreme cruelty or profanity. Cruelty is defined as: physical or emotional acts against any animal or person that are primarily intended to hurt or inflict pain. Topic includes obscene words, phrases, and profanity in either audio, text, or pictures.

Search Engines

Search engine sites such as AltaVista, InfoSeek, Yahoo!, and WebCrawler.

Sports and Leisure

Pictures or text describing sporting events, sports figures, or other entertainment activities.

Sex Education

Pictures or text advocating the proper use of contraceptives. Topic includes sites devoted to the explanation and description of condoms, oral contraceptives, intrauterine appliances, and other types of contraceptives. It also includes discussion sites devoted to conversations with partners about sexually transmitted diseases, pregnancy, and sexual boundaries. Not included in this category are commercial sites selling sexual paraphernalia (topics included under *Sexual Acts*).

Sexual Acts

Pictures or text exposing anyone or anything involved in explicit sexual acts and/or lewd and lascivious behavior. Topic includes masturbation, copulation, pedophilia, as well as intimacy involving nude or partially nude people in heterosexual, bisexual, lesbian, or homosexual encounters. It also includes phone sex advertisements, dating services, adult personals, and sites devoted to selling pornographic CD-ROMs and videos.

Full Nudity

Pictures exposing any or all portions of human genitalia. Topic does *not* include sites categorized as Partial/Artistic Nudity containing partial nudity of a wholesome nature. For example, it does not include Web sites for publications such as *National Geographic* or *Smithsonian* magazine nor sites hosted by museums such as the Guggenheim, the Louvre, or the Museum of Modern Art.

Partial/artistic Nudity

Pictures exposing the female breast or full exposure of either male or female buttocks except when exposing genitalia which is handled under the Full Nudity category. Topic does not include swimsuits, including thongs.

Troubleshooting Tips

The following information is offered to help overcome any difficulties that might occur when installing and setting up your SOHO 6.

General

What do the PWR, Status, and Mode lights signify on the SOHO 6?

When the PWR light is lit, the SOHO 6 has power. When the Status light is lit, there is a management connection to the SOHO 6. When the MODE light is lit, the SOHO 6 is operational.

If the PWR light is *blinking*:

The SOHO 6 is running from its backup flash memory. You are able to connect to the SOHO 6 from a computer on one of the

four, numbered, Ethernet ports (labeled 0-3) and reload the configuration.

If the Mode light is *blinking*:

The SOHO 6 requires a DHCP assigned IP address for the external interface, but did not receive it. The WAN port is not connected to another appliance, the physical connection is faulty, or the other appliance is not operating properly.

How do I register my SOHO 6 with the LiveSecurity Service?

Register online by activating your bundled LiveSecurity® Service subscription. Activation entitles you to receive threat alert notifications, expert security advice, free anti-virus protection, software updates, technical support by web or phone, and access to extensive online help resources. To activate, make a note of your SOHO serial number, then use your Web browser to go to:

<http://www.watchguard.com/activate>

For more information, see “Register your SOHO 6 and Activate the LiveSecurity Service” on page 27.

How do I restart my SOHO 6?

- 1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: <http://192.168.111.1>
- 2 Click **Reboot**.
- 3 Wait for the SOHO 6 to complete the process. The MODE light on the front of the SOHO 6 will turn off, then back on. The SOHO 6 takes 30 seconds to boot up.

NOTE

You can also reboot by removing the power source for ten seconds, and then restoring power.

How do I reset my System Security password, if I forgot or lost it?

If you forgot your password, you must reset the SOHO 6 to its factory default. For instructions, see “Reset a SOHO 6 to factory default” on page 26.

How does the seat limitation on the SOHO 6 work?

The default user license on the SOHO 6 allows for ten users. The first ten computers on the network behind the SOHO 6 to access the Internet are allowed through the SOHO 6. To clear the list of these first ten computers you *must* reboot the SOHO 6.

What is a SOHO 6 Feature Key?

The Feature Key is an encrypted mask that tells the SOHO 6 which features are active. It is obtained by redeeming an upgrade option license key at the LiveSecurity Service Web site. You copy the Feature Key into a SOHO 6 configuration page and it is then stored in memory. For further instruction, see “Redeem your SOHO 6 Upgrade Options” on page 57.

I can't get a certain SOHO 6 feature to work with a DSL modem.

Some DSL routers implement NAT firewalls. Running NAT in front of the SOHO 6 causes problems with WebBlocker and the performance of IPSec. When a SOHO 6 is used in conjunction with

a DSL router, set the NAT feature of the DSL router to bridge-only mode.

How do I install and configure the SOHO 6 using a Macintosh (or other) operating system?

Installation instructions for the Macintosh and other operating systems are on the WatchGuard Web site at:

<https://support.watchguard.com/sohoresources/>

How do I know whether the cables are connected correctly to my SOHO 6?

There are fourteen lights on the front of the SOHO 6 grouped in pairs. The link light labeled WAN tells you if your SOHO 6 is connected to your modem. If this light is not lit, the SOHO 6 is not connected to your modem. Check to make sure that both sides of the cable are connected and that your Internet connection is active. The link lights labeled 0 through 3 correspond to the four numbered Ethernet ports of the trusted network. They tell you if the SOHO 6 is connected to a computer or hub. If the lights are not lit, the SOHO 6 is not connected to the computer or hub. Check to make sure that both sides of the cable are connected and that the computer or hub has power.

I can connect to the configuration screen; why can't I browse the Internet?

This means that the SOHO 6 is on, but something is wrong with the connection from the SOHO 6 to the Internet. Make sure the cable or DSL modem is connected correctly and has power. Also check the link light on your modem as well as the WAN link light on the SOHO 6.

If you continue to have trouble connecting to the Internet, call your ISP.

How can I see the MAC address of my SOHO 6?

A MAC (Media Access Control) address is a unique number used to identify the actual physical hardware of an Ethernet appliance.

- 1 With your Web browser, go to the SOHO 6 Configuration Settings page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: <http://192.168.111.1>
- 2 Towards the bottom of the System Status page, you see the External network header on the right side. Two MAC addresses are often listed.
Please note these addresses and have them ready if you need Technical Support.

Configuration

Where are the SOHO 6 settings stored?

The configuration parameters are stored in memory on the SOHO 6.

How do I set up DHCP on the trusted network of the SOHO 6?

- 1 Make sure your computer is set up to use DHCP. For instructions, see “Enable your computer for DHCP” on page 16.
- 2 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: <http://192.168.111.1>
- 3 From the navigation bar on the left side, select **Network ⇒ Trusted**.
- 4 Select **Enable DHCP Server** and then click **Submit**.

How do I change to a static, trusted IP address?

Before you can use a static IP address, you must have a base Trusted IP address and subnet mask.

The following IP address ranges and subnet masks are set aside for private networks in compliance with RFC 1918. Replace the Xs in the network IP address with a number between 1 and 254. The subnet addresses do not need to be changed.

Network IP range	Subnet mask
10.x.x.x	255.0.0.0
172.16.x.x	255.240.0.0
192.168.x.x	255.255.0.0

To change to a static, trusted IP address:

- 1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: <http://192.168.111.1>
- 2 From the navigation bar on the left side, select **Network ⇒ Trusted**.
- 3 Disable **Enable DHCP Server** and then click **Submit**.
- 4 Enter the information. Click **Submit**.

How do I set up and disable Webblocker?

- 1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: <http://192.168.111.1>
- 2 From the navigation bar on the left side, select **WebBlocker ⇒ Settings**.
The WebBlocker Settings page appears.
- 3 Select **Enable WebBlocker**. Enter a full access password, and an inactivity timeout (in minutes).

To disable WebBlocker, deselect **Enable WebBlocker**.

How do I allow incoming services such as POP3, Telnet, and Web (HTTP)?

- 1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: `http://192.168.111.1`
- 2 From the navigation bar on the left side, select **Firewall ⇒ Incoming**.
The Filter Incoming Traffic page appears.
- 3 Locate the pre-configured service you wish to allow in and select **Allow** from the drop list.
- 4 Enter the Trusted network IP address of the computer hosting the service.
- 5 Click **Submit**.

How do I allow incoming IP, or uncommon TCP and UDP protocols?

You need the IP address of the computer that is receiving the incoming data and the IP protocol number that corresponds to the specific incoming IP protocol. To allow an incoming IP protocol:

- 1 With your Web browser, go to the System Status page using the Trusted IP address of the SOHO 6.
For example, if using the default IP address, go to: `http://192.168.111.1`
- 2 From the navigation bar on the left side, select **Firewall ⇒ Custom Service**.
The Custom Service page appears.
- 3 Beneath the Protocol Settings fields, select **TCP Port, UDP Port** or **Protocol** from the drop list.
The Custom Service page refreshes.
- 4 Enter a name for the service.

- 5 Enter the protocol number to allow in the Protocol field.
- 6 Click **Submit**.
- 7 From the navigation bar on the left side, select **Firewall** ⇒ **Incoming**.
The Firewall Incoming Traffic page appears.
- 8 Near the bottom of the page, under the Custom Service header, locate the service you created and select **Allow** from the drop list.
- 9 Under the header Service Host, enter the IP address of the computer to which this traffic is allowed.
- 10 Click **Submit**.

VPN Management

Before setting up VPN, you must have:

- Two properly configured and working SOHO 6s or one SOHO 6 with the latest version of firmware and one Firebox II/III. Each SOHO 6 must have the VPN option activated.
- The static external IP address, the network address, and the subnet masks of both appliances. (The base trusted IP address of each SOHO 6 must be static and unique.)
- The DNS and WINS server IP address, if used.
- The shared key (passphrase) for the tunnel.
- The same encryption method for each end of the tunnel (DES or 3DES).
- The same authentication method for each end (MD-5 or SHA-1).

How do I set up my SOHO 6 for VPN Manager Access?

This requires the add-on product, WatchGuard VPN Manager software, which is purchased separately and used with the WatchGuard Firebox System software. To purchase VPN Manager, use your Web browser to go to:

<https://www.watchguard.com/products/vpnmanager.asp>

For more information on how to allow VPN Manager access to a SOHO 6, see the *VPN Guide*.

How do I set up VPN to a SOHO 6s?

For detailed information on how to configure a VPN tunnel between a SOHO 6 and another IPSec compliant appliance, use your Web browser to go to:

https://support.watchguard.com/AdvancedFaqs/sointerop_main.asp

- 1 Log in to the site.
- 2 Download the file you need.
- 3 Follow the instructions to configure your VPN tunnel.

Contact Technical support

(877) 232-3531	U.S.; End-user support
(206) 521-8375	U.S.; Authorized Reseller support
(360) 482-1083	International support

Online Documentation and In-Depth FAQs

WatchGuard maintains an extensive knowledge base consisting of product documentation in the form of printer friendly .pdf files, tutorials, In-Depth FAQs, and more. This information is available at:

<https://support.watchguard.com/AdvancedFaqs/>

Index

Numerics

100 indicator 7

A

Add Route page 41

B

blocked sites
 configuring 65
Blocked Sites page 66
browsers, supported 12
button, RESET 8

C

cables
 correct setup 110
 included in package 2
 required 12
configuration file, viewing 24, 60
custom incoming services, creating 63
Custom Service page 64, 113

D

default factory settings 25–26
DHCP
 described 32
 setting up on Trusted Network 111
DNS service, dynamic 43
DSL modems, and SOHO 6 109
Dual ISP Port 44

Dynamic DNS client page 43
dynamic DNS service,
 configuring 43–44, ??–47
Dynamic Host Configuration Protocol.
 See DHCP
dynamic IP addresses
 configuring for 32
 described 31

E

events
 described 75
 logging, See logging
External Network
 denying ping packets received
 on 68

F

FAQs 116
feature keys 57, 109
filter rules, specifying for custom
 services 65
Filter Traffic page 62
Firewall Incoming Traffic page 114
Firewall Options page 67
firewall, specifying miscellaneous
 options 67
firmware
 updating 56
 viewing version of 24
FTP access, denying to the Trusted
 interface 68

G

Groups page 101

H

hardware description 6
HTTP proxy settings, disabling 14

I

incoming service, creating custom 63
indicators
 100 7
 link 7
 Mode 7
 WAN 7
installation
 cabling 19
 cabling for multiple computers 20
 determining TCP/IP settings 12
 disabling TCP/IP proxy
 settings 14
 items required for 12
Internet
 how information travels on 4
 problems browsing 110
IP addresses
 described 4
 disguising 5
 dynamic 31
 in networks 31
 maintaining table of 85

L

license keys, redeeming 57
licenses, upgrading 21
lights
 100 7
 link 7
 MODE 107
 Mode 7
 power 6
 PWR 107
 Status 7, 107, 108
 WAN 7
link indicator 7

LiveSecurity Service
 registering with 27
 renewing subscription 59
log host, setting WSEP 77
log messages
 contents of 76
 synchronizing with computer 77
 viewing 76
logging
 described 75
 to a WSEP host 77
 to Syslog host 79
Logging page 76

M

MAC address of SOHO 6 111
MacIntosh operating system 110
Mode indicator 7
MODE light 107
MUVPN clients option 93
MUVPN, license keys for 59

N

NAT 5
Network Address Translation (NAT) 5
Network Statistics page 42
network statistics, viewing 42
New User page 102
numbered ports 9

O

OPT port 8

P

pages
 Add Route 41

- Blocked Sites 66
- Custom Service 64, 113
- Dynamic DNS client 43
- Filter Traffic 62
- Firewall Incoming Traffic 114
- Firewall Options 67
- Groups 101
- Logging 76
- Network Statistics 42
- New User 102
- Routes 41, 46, 48
- SOHO 6 Administration 51
- Syslog Logging 79
- System Security 52, 53
- System Status 23, 28
- System Time 81
- Unrestricted Pass Through IP Address 72
- Update 56
- Upgrade 58
- View Configuration File 60
- VPN Manager Access 55
- VPN Statistics 94
- WatchGuard Security Event Processor 78
- WebBlocker Groups 100
- WebBlocker Settings 98
- Pass Through feature 72
- passphrases
 - described 52
 - setting up 53, 54
- ping packets, denying all 68
- Point-to-Point Protocol over Ethernet.
 - See PPPoE
- ports
 - numbered 9
 - numbers 5
 - OPT 8
 - WAN 9
- power input 9
- PPPoE
 - configuring for 34
 - described 32
- pre-configured services, adding 62
- protocols
 - allowing incoming 113
 - described 4

PWR light 6, 107

R

- rebooting 28
- rebooting on remote system 29
- registration 27
- Remote Management 54
- RESET button 8
- resetting to factory default 26
- Routes page 41, 46, 48
- routes, configuring static 40

S

- seat licenses, upgrading 58
- seat limitation 109
- serial number, viewing 24
- services
 - adding incoming 62
 - adding pre-configured 62
 - allowing incoming 113
 - and security risks 62
 - creating custom 63–65
 - creating custom incoming 63
 - described 5, 61
 - preconfigured 62
 - specifying filter rule for 65
- sites
 - blocking 65
- SOCKS
 - configuring application 69
 - configuring for SOHO 6 68
 - described 68
 - disabling 70
- SOHO 6 28, 29
 - and DSL modems 109
 - and MacIntosh operating system 110
 - and SOCKS 68
 - base model 27
 - configuring access to 51
 - configuring for dynamic addresses 32

- configuring for PPPoE 34
- configuring for static
 - addressing 33
- configuring VPN tunnel with 86
- connecting to 23
- default factory settings 25
- described 2
- firewall feature 67
- front view 6
- function of 3
- hardware 6
- installing 11–22
- MAC address of 111
- MUVPN clients option 93
- package contents 2
- ports 6, 8
- rear view 8
- registering 27
- resetting to factory default 26
- seat limitation 109
- setting passphrase 53
- setting up VPNs between 115
- troubleshooting 107–115
- upgrading 57
- upgrading user license 21
- viewing log messages for 76

SOHO 6 Administration page 51

SOHO Remote Management 54

Split Tunneling 93

static IP addresses

- and VPNs 87
- obtaining 87

static IP addressing, configuring

- for 33

static routes, configuring 40

Status light 7, 107, 108

Syslog Logging page 79

System Security page 52, 53

System Status page 23, 28

System Time page 81

system time, setting 80

T

TCP/IP settings, determining 12–14

technical support 116

time, setting 80

traffic

- creating unrestricted pass through 72
- logging all outbound 70

traffic, monitoring 42

troubleshooting 107–115

Trusted Network

- configuring additional computers on 38
- denying FTP access to 68

Trusted Network Configuration

- page 37, 39

U

Unrestricted Pass Through IP Address

- page 72

Update page 56

Update Wizard 57

upgrade license keys

- redeeming 57
- types of 58

Upgrade page 58

upgrading

- seat licenses 58
- user licenses 21
- VPNs 59

V

View Configuration File page 60

VPN Manager

- described 54
- purchasing 115
- setting up access to 54–55
- setting up SOHO 6 for 115

VPN Manager Access page 55

VPN Statistics page 94

VPN upgrade

- enabling 86
- obtaining 88

VPNforce™ Port 47
VPNs
 and SOHO 6, SOHO 6 tc 2
 and static IP addresses 87
 between two SOHO 6s 115
 configuring with SOHO 6 86–88
 described 83
 enabling tunnels 88
 encryption for 87
 license key for 59
 requirements for 84, 114
 special considerations for 87
 troubleshooting connections 88
 viewing statistics 94

W

WAN indicator 7
WAN port 9
WatchGuard Security Event
 Processor 77
WatchGuard Security Event
 Processor page 78
WebBlocker
 activating 98
 categories 103–??
 configuring 98
 creating users and groups for 99
 database 95
 described 95
 enabling and disabling 112
 purchasing and activating 97
 users and groups 97
WebBlocker Groups page 100
WebBlocker Settings page 98
WebBlocker upgrade, purchasing 97
WebBlocker, license key for 59
WSEP 77

