

# WatchGuard® SOHO User Guide

---

SOHO and SOHO|tc version 5.0



---

WatchGuard SOHO and SOHO | tc



---

## Using this guide

---

This guide assumes that you are 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 throughout this guide.

---

<b>Convention</b>	<b>Indication</b>
<b>Bold</b> type	Denotes menu commands, dialog box options, Web page options, Web page names. For example: "On the System Information page, select Disabled."
<b>CAUTION</b>	Denotes a warning or precautionary information.
<b>NOTE</b>	Denotes important information, a helpful tip, or additional instructions.

---

---

## Certifications and Notices

---

### FCC Certification

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

Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device 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 brouleur du Canada.

---

## Taiwanese Notice

**警告使用者：**

這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

## 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):**

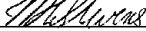
Internet Firewall, Model WG2500

**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 Mark Stevens  
Position Senior VP Perimeter Security  
Date 29 August 2001

---

# WatchGuard® End-User License Agreement

---

## IMPORTANT - READ CAREFULLY BEFORE ACCESSING WATCHGUARD SOFTWARE

This WatchGuard 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 software product you have purchased, which includes computer software and any separately installed components, and any updates or modifications thereto, and which may include associated media, printed materials, and on-line or electronic documentation (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 suppliers. 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 install and use the SOFTWARE PRODUCT on any computer with an associated connection to the hardware product (the “Hardware”); (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 each computer on which you install the SOFTWARE PRODUCT has an associated connection to the Hardware; 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 WATCHGUARD or the authorized dealer from whom you obtained the SOFTWARE PRODUCT 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 your authorized dealer will provide you with a new version of the SOFTWARE PRODUCT or a full refund at its 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 OR 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 OR ITS LICENSORS 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 AND THE LIABILITY OF ITS LICENSORS (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 SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF AN AGREED REMEDY. IN NO EVENT WILL WATCHGUARD OR ITS LICENSORS 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 AND ITS LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF



---

SUCH DAMAGES. THIS SHALL 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 DFARS 227.7202-3 (Commercial Computer Software) and DFARS 252.227-7015(b) (Technical Data-Commercial Items) -- Restricted Rights Clause at FAR 52.227-19, as applicable. Manufacturer is WatchGuard Technologies, Incorporated, 505 Fifth Avenue, South, Suite 500, Seattle, WA 98104.

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

7. TERMINATION. This license and your right to use the SOFTWARE PRODUCT will automatically terminate 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 contents of this package AND BY USING THE SOFTWARE PRODUCT YOU AGREE TO THESE TERMS. No change or modification of this EULA will be valid unless it is in writing, and is signed by WATCHGUARD.

9. CANADIAN TRANSACTIONS. If you obtained this SOFTWARE PRODUCT in Canada, you agree to the following: The parties hereto have expressly required that the present EULA be drawn up in the English language. / Les parties aux presentes ont expressement exige que la presente conventions et ses Annexes soient redigees en la langue anglaise.

---

## WatchGuard® Limited Hardware Warranty

---

This WatchGuard Limited Hardware Warranty (the "Warranty") applies to the enclosed WatchGuard hardware product (the "Hardware Product"). By using the HARDWARE Product, you agree to the terms hereof. If you do not agree to these terms, please return this package, along with proof of purchase, to the authorized dealer from whom you purchased the Hardware Product for a full refund. THIS WARRANTY DOES NOT APPLY TO THE WATCHGUARD SOFTWARE REQUIRED FOR OPERATION AND USE OF THE HARDWARE PRODUCT. PLEASE REFER TO THE ENCLOSED WATCHGUARD END-USER LICENSE AGREEMENT (THE "EULA") FOR THE SOFTWARE WARRANTY AND OTHER TERMS AND CONDITIONS ASSOCIATED WITH USE OF THE SOFTWARE. IF YOU DO NOT AGREE TO THE TERMS OF THE EULA, PLEASE RETURN THIS PACKAGE IN ACCORDANCE WITH THIS PARAGRAPH.

NOW, THEREFORE, WatchGuard Technologies and you agree as follows:

1. **Limited Warranty.** WatchGuard Technologies warrants that upon delivery and for one (1) year thereafter (as the same may be extended pursuant to Section 2 below, the "Warranty Period"): (a) the Hardware Product will be free from material defects in materials and workmanship, and (b) the Hardware Product, when properly installed and used for its intended purpose and in its intended operating environment, will perform substantially in accordance with WatchGuard Technologies applicable specifications. This warranty does not apply to any Hardware Product that has been: (i) altered, repaired or modified by any party other than WatchGuard Technologies; or (ii) damaged or destroyed by accidents, power spikes or similar events or by any intentional, reckless or negligent acts or omissions of any party. You may have additional warranties with respect to the Hardware Product from the manufacturers of Hardware Product components. However, you agree not to look to WatchGuard Technologies for, and hereby release WatchGuard Technologies from any liability for, performance of, enforcement of, or damages or other relief on account of, any such warranties or any breach thereof.
2. **Remedies.** If any Hardware Product does not comply with WatchGuard Technologies warranties set forth in Section 1 above, WatchGuard Technologies will, at its option, either (a) repair the Hardware Product, or (b) replace the Hardware Product; provided, that you will be responsible for returning the Hardware Product to the place of purchase and for all costs of shipping and handling. As to any Hardware Product repaired or replaced by WatchGuard Technologies, the Warranty Period will end one (1) year after delivery of the repaired or replacement Hardware Product. Any Hardware Product, component, part or other item replaced by WatchGuard Technologies becomes the property of WatchGuard Technologies. WatchGuard Technologies shall not be responsible for return of or damage to any software, firmware, information or data contained in, stored on, or integrated with any returned Hardware Products.
3. **Disclaimer and Release.** THE WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD TECHNOLOGIES, AND YOUR REMEDIES, SET FORTH IN PARAGRAPHS 1 AND 2 ABOVE ARE EXCLUSIVE AND IN SUBSTITUTION FOR, AND YOU HEREBY WAIVE, DISCLAIM AND RELEASE ANY AND ALL OTHER WARRANTIES, OBLIGATIONS AND LIABILITIES OF WATCHGUARD TECHNOLOGIES AND ALL OTHER RIGHTS, CLAIMS AND REMEDIES YOU MAY HAVE AGAINST WATCHGUARD TECHNOLOGIES, EXPRESS

---

OR IMPLIED, ARISING BY LAW OR OTHERWISE, WITH RESPECT TO ANY NONCONFORMANCE OR DEFECT IN THE HARDWARE 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 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 TECHNOLOGIES AND ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY FOR LOSS OR DAMAGE TO, OR CAUSED BY OR CONTRIBUTED TO BY, THE HARDWARE PRODUCT).

4. **Limitation of Liability.** WATCHGUARD TECHNOLOGIES' liability (WHETHER ARISING IN CONTRACT (INCLUDING WARRANTY), TORT (INCLUDING ACTIVE, PASSIVE OR IMPUTED NEGLIGENCE AND STRICT LIABILITY AND FAULT) OR OTHER THEORY) with regard to any HARDWARE Product will in no event exceed the purchase price paid by you for such HARDWARE Product. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF AN AGREED REMEDY. IN NO EVENT WILL WATCHGUARD TECHNOLOGIES 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) OR OTHER THEORY, FOR COST OF COVER OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION OR DATA) ARISING OUT OF OR IN CONNECTION WITH THIS WARRANTY OR THE USE OF OR INABILITY TO USE THE HARDWARE PRODUCT, EVEN IF WATCHGUARD TECHNOLOGIES HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS SHALL BE TRUE EVEN IN THE EVENT OF THE FAILURE OF AN AGREED REMEDY.

5. **Miscellaneous Provisions.** This Warranty will be governed by the laws of the state of Washington, without reference to its choice of law rules. The provisions of the 1980 United Nations Convention on Contracts for the International Sale of Goods, as amended, shall not apply. If any provision of this Warranty is found to be invalid or unenforceable, then the remainder shall have full force and effect and the invalid provision shall be modified or partially enforced to the maximum extent permitted by law to effectuate the purpose of this Warranty. This is the entire agreement between WatchGuard Technologies and you relating to the contents of this package, and supersedes any prior purchase order, communications, advertising or representations concerning the contents of this package AND BY USING THE HARDWARE PRODUCT YOU AGREE TO THESE TERMS. No change or modification of this Agreement will be valid unless it is in writing, and is signed by WatchGuard Technologies.

---

## Copyright and Patent Information

---

Copyright © 1999-2001 WatchGuard Technologies, Inc. All rights reserved.

WatchGuard and LiveSecurity are either registered trademarks or trademarks of WatchGuard Technologies, Inc. in the United States and other countries. Firebox is a trademark of WatchGuard Technologies, Inc.

CyberPatrol is a registered trademark of SurfControl, Inc.

DocVer: B-2.4-User-2

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

---

# Table of Contents

---

CHAPTER 1 Introduction .....	17
Registration and Identification Information .....	18
How does a firewall work? .....	18
How does information travel on the internet? .....	20
How does the SOHO process this information? .....	21
The SOHO Home Page—System Status .....	22
The Default Factory Settings .....	22
Rebooting a WatchGuard SOHO .....	24
CHAPTER 2 Getting Started .....	27
Before you begin .....	27
The Installation Process .....	28
CHAPTER 3 Setting Up Your SOHO Network .....	37
Configuring Your External Network .....	37

---

Configuring Your Trusted Network .....	47
Configuring Static Routes .....	49
View the Network Statistics .....	50
CHAPTER 4 Your Administrative Options .....	53
The System Security Page .....	53
Setting up VPN Manager Access .....	56
Update Your Configuration from a Non-Windows Platform .....	58
Redeeming your SOHO upgrade certificates .....	58
View the Configuration File .....	61
CHAPTER 5 Configuring Your Firewall Settings .....	63
Firewall settings .....	63
Configuring Incoming and Outgoing Services .....	63
Blocking External Sites .....	67
Firewall Options .....	69
Creating a virtual DMZ .....	74
CHAPTER 6 What is Logging? .....	77
Viewing SOHO log messages .....	77
Setting a WatchGuard Security Event Processor log host .....	78
Setting a Syslog Host .....	80
Setting the System Time .....	81
CHAPTER 7 WatchGuard SOHO WebBlocker .....	85
How WebBlocker works .....	85
Purchasing and enabling SOHO WebBlocker .....	87

---

Configuring the SOHO WebBlocker .....	88
WebBlocker categories .....	93
Searching for blocked sites .....	96
CHAPTER 8 Configuring Virtual Private Networking ..	97
What you will need .....	98
Step-by-step instructions for configuring a SOHO VPN tunnel .....	100
Frequently asked questions .....	101
MUVPN Clients .....	103
View the VPN Statistics .....	103
CHAPTER 9 Resources .....	105
Troubleshooting .....	105
Contacting Technical support .....	114
Online Documenting and In-Depth FAQs .....	114
Special Notices .....	114





# Introduction

---

## Welcome

---

Congratulations on purchasing the ideal solution for providing secure access to the Internet—the WatchGuard SOHO or WatchGuard SOHO | tc. Your new security device will give you peace of mind when connecting to the Internet using a high-speed cable or DSL modem, a leased line, or ISDN.

This User Guide applies to both the SOHO and the SOHO | tc—the name SOHO is used to refer to both these devices throughout the guide. The only difference between them is the ability to create and use a Virtual Private Network (VPN). This VPN option can be added to the SOHO, while the SOHO | tc comes with the VPN option already installed.

The most current installation and user information is available on the Internet at:

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

## Registration and Identification Information

---

Once you have installed and configured your SOHO following the instructions you will find in the upcoming chapters, you will need to register the unit at our Web site. When the registration is complete you can take advantage of our LiveSecurity service as well as any upgrade options you may have purchase.

Please use this area, provided for your convenience, to enter your SOHO information.

SOHO Serial Number:	
LiveSecurity User ID:	
Password:	

The SOHO serial number is located on the bottom of the SOHO unit. You create a LiveSecurity user ID and password when you register your WatchGuard SOHO or SOHO | tc.

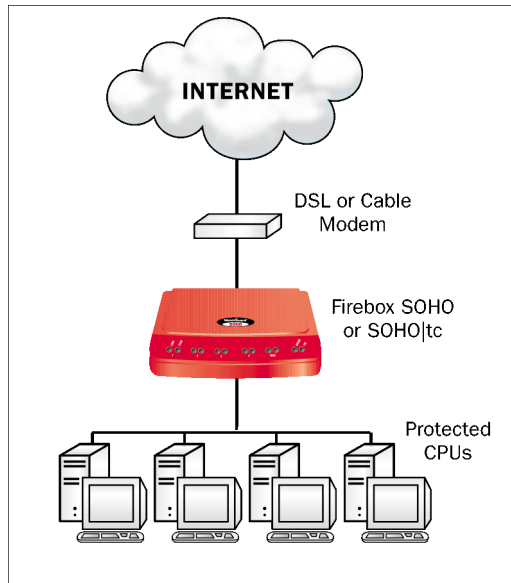
Please keep this information in a secure place.

## How does a firewall work?

---

Fundamentally, a firewall is a way of differentiating between, as well as protecting, “us” from “them”. On the external side of your SOHO firewall is the entire Internet. The Internet has many resources that you want to be able to reach, such as the Web, Email, and video/audio conferencing. It also presents dangers to the privacy and security of your computers. On the trusted side of your SOHO firewall are all the devices you want to protect from

these dangers. As is illustrated in the image below, the SOHO physically separates your trusted network from the Internet.



Using rules we will discuss in Chapter 3: “Configuring Incoming and Outgoing Services” on page 63, the WatchGuard SOHO evaluates all traffic between the external network (the Internet) and the trusted network (your computers) and blocks any suspicious activity. In order for this to work as described, you must configure both the external and trusted networks to work together and to talk to one another as well as the rest of the world.

## **How does information travel on the internet?**

---

Each packet of information transported over the Internet must be packaged in a special way to ensure that it is able to travel from one computer to the next. A system called Internet Protocol (IP) takes chunks of information and wraps them up with a header identifying both where the information is going and how it should be handled enroute.

### **IP Addresses**

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

On the Internet, IP addresses can be identified using either a string of numbers or a user-friendly domain name. For example, the IP address of the WatchGuard site is 209.191.160.60 while the domain name is [www.watchguard.com](http://www.watchguard.com).

### **Protocol**

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

### **Port number**

The port number alerts the computers at both the sending and receiving end how to handle the packet.

## **How does the SOHO process this information?**

---

### **Services**

A service is the combination of protocol(s) and port numbers associated with a specific application or communication type. To facilitate configuration of your SOHO, WatchGuard lets you select pre-configured versions of several commonly used services.

### **Network Address Translation (NAT)**

All incoming connections through a SOHO automatically use a feature called dynamic network address translation (dynamic NAT). Without dynamic NAT, your trusted, private addresses would not be passed along the Internet to their destination.

Furthermore, the SOHO protects your trusted network by disguising private IP addresses. During an Internet connection, all traffic passed between computers includes their IP address information. However, due to the dynamic NAT feature, applications and servers on the Internet only see the public, external IP address of the SOHO itself and are never privy to the addresses in your trusted network address range when they exchange information with a computer behind your firewall.

Imagine that you install a computer behind the SOHO with the private IP address 192.168.111.12. If this address were broadcast to the Internet, hackers could easily direct an attack on the computer itself. Instead, the SOHO converts the address automatically to the public, external address of the SOHO. When a hacker tries to violate the computer, they are stopped cold at the SOHO, never learning the true address of your computer.

## The SOHO Home Page—System Status

---

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

- The firmware version
- A few of the SOHO features and their status:
  - WSEP Logging
  - VPN Manager
  - Syslog
  - DMZ
- Upgrade options and their status
- Configuration information for both the Trusted and External networks
- Configuration information on your firewall settings (that is, Incoming and Outgoing services)
- A reboot button to restart the unit

## The Default Factory Settings

---

Your SOHO 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 onboard configuration pages are available to all on the trusted network.
- SOHO 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 certificates have been redeemed.

## **Resetting a SOHO to the Factory Defaults**

It is possible that due to a firmware corruption or other unforeseen misfortune (such as a lost System Security passphrase) you may need to reset the SOHO to the factory defaults.

To do this, you will need to remove the SOHO from your network disconnect the power, disconnect all cables, plug one end of an Ethernet cable into the WAN port in the back of the device and the other end into any of the other four (numbered 1-4) Ethernet ports. Then, reconnect the power, wait at least 90 seconds, and disconnect power. Your SOHO is now reset to factory defaults. Connect the cables in the original configuration and power up again.

## The Base Model SOHO

The base model SOHO comes with a ten seat license, that is ten computers have access to the Internet through the SOHO. Remember, while only four devices connect directly to the four (numbered 1-4) Ethernet ports, one or more of these devices can be a hub or router. Please see, "Cabling the SOHO for more than four computers" on page 34.

## Rebooting a WatchGuard SOHO

---

To reboot a SOHO located on a local system, use one of the following methods:

- Using your Web browser.  
With your Web browser, go to the SOHO System Status page using the Trusted IP address of the SOHO. (For example, if using the default IP address, go to: <http://192.168.111.1>.)  
Click the **Reboot** button.
- Unplug the SOHO and plug it back in.

To reboot a SOHO located on a remote system, the SOHO must be configured to allow either incoming Web or FTP traffic to the trusted address of the SOHO. For information on configuring a SOHO to allow incoming traffic, see "Configuring Incoming and Outgoing Services" on page 63.

You can than use one of the following methods:

- Open a special HTML page with the external IP address of the SOHO in the URL followed by `/rebootreq`. For example, <http://209.191.160.60/rebootreq>.



- Send an FTP command to the remote SOHO device. Use an FTP application to connect to the SOHO device, then enter the command: `quote rebt`



# Getting Started

---

## Before you begin

---

### Pre-installation checklist

Before installing your new WatchGuard SOHO please ensure that you have:

- A 10BaseT Ethernet I/O network card installed in your computer.
- A cable or DSL modem with a 10BaseT port.
- Two Ethernet network cables with RJ45 connectors. These must *not* be “crossover cables” (which are usually red or orange). One cable is furnished with your unit. A second cable may have been supplied with your modem. If not, you will need to purchase a second Ethernet, RJ45 cable. Make sure that both cables are long enough to comfortably connect the modem to the SOHO and the SOHO to the computer in your individual office environment.

- An operational Internet connection. Setup of your SOHO requires access to the Internet. If your connection does not work, please contact your Internet service provider (ISP). When your connection has been established, you may proceed with installation and setup.
- If you have either a cable or DSL modem, consult the manual that came with your service, or call the ISP to find out whether your particular modem supports DHCP or PPPoE. You will need this information later in the installation process.
- If you are using PPPoE to connect to your local Internet service provider, the WatchGuard SOHO must be running firmware version 2.0 or later.
- An installed Web browser—either Netscape Navigator 4.77 (or higher) or Internet Explorer 5.0 (or higher).
- SOHO serial number.

## The Installation Process

---

Before you begin the installation process, connect to the Internet. You need to determine your current TCP/IP settings and disable your HTTP proxy.

---

### **NOTE**

You must also know whether your ISP provides you with Dynamic or Static TCP/IP settings. For assistance, please see, "Determining whether your ISP uses dynamic or static addressing" on page 38.

---

## Determine your current TCP/IP settings

For your reference, record the computer's current TCP/IP settings in the chart provided at the end of this section. Different operating systems will supply different information. To locate your settings:

### Microsoft Windows NT or 2000

- 1 Click **Start** ⇒ **Programs** ⇒ **Command Prompt**.
- 2 At the C:\ prompt, enter `ipconfig/all`. Press **Enter**.
- 3 Enter your current TCP/IP settings in the chart provided below.
- 4 Click **Cancel**.

### Microsoft Windows 95 or 98 or ME

- 1 Click **Start** ⇒ **Run**.
- 2 Type: `winipcfg`. Click **OK**.
- 3 Select the "Ethernet Adapter."  
Enter your current TCP/IP settings in the chart provided below.
- 4 Click **Cancel**.

### Macintosh

- 1 Click **Apple menu** ⇒ **Control Panels** ⇒ **TCP/IP**.
- 2 Enter your current 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 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	
Primary WINS Server		.	.	.
Secondary WINS Server		.	.	.
DNS Server(s)	Primary	.	.	.
	Secondary	.	.	.

---

**NOTE**

If you are connecting more than one computer to the trusted network behind the SOHO, obtain the configuration TCP/IP information for each computer.

---

## Disable your browser's HTTP proxy

To configure a WatchGuard SOHO after it is installed, you must be able to access the special configuration pages that reside on the SOHO. If the HTTP proxy in your browser is enabled, you can not access these pages, and you can not 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 will not prevent you from accessing your favorite Web sites, but it will allow you to access the special configuration pages that reside only on the SOHO.

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.

### **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 6/6.1**

- 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 arrow 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.

### **Internet Explorer 5.0/5.5 and 6.0**

- 1 Open Internet Explorer.
- 2 Click **Tools** ⇒ **Internet Options**.  
The Internet Options screen displays.
- 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.

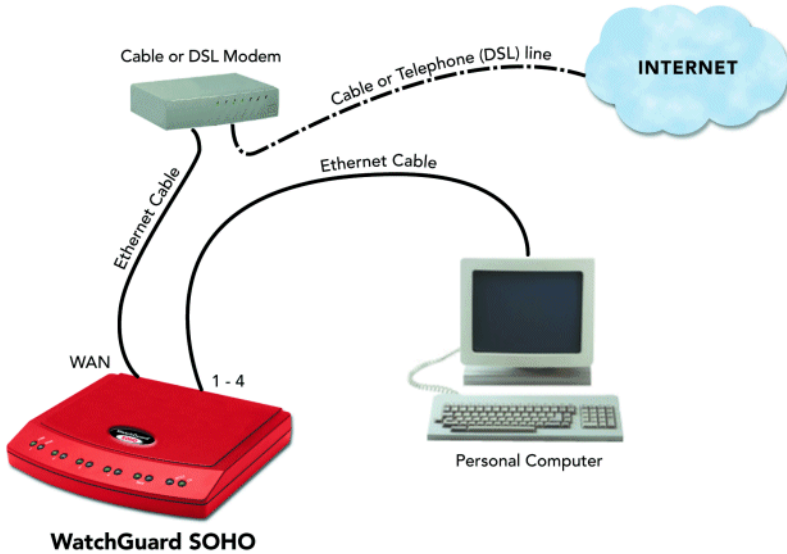
### **Physically connecting your SOHO**

Your WatchGuard SOHO can be used to protect a single computer or a multi-computer network. It can also function as a hub to connect a variety of other devices.

#### **Cabling the SOHO for one to four devices**

The SOHO has four (numbered 1-4) Ethernet ports. Each can be used to connect a variety of devices. These may include computers, printers, scanners, or other network peripherals. Your SOHO may replace an existing hub if you have no more than four devices to connect.



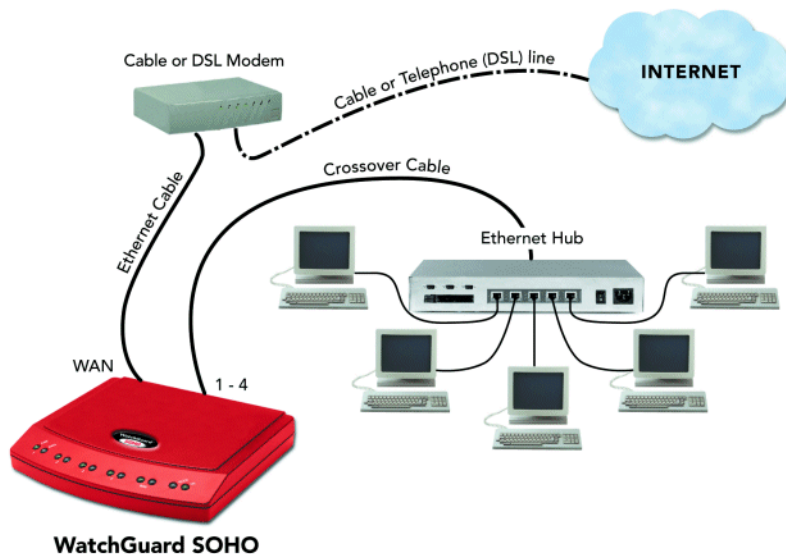


- 1 Complete the “Pre-installation checklist” on page 27.
- 2 Shut down your computer and unplug the power from your DSL or cable modem.
- 3 Unplug the Ethernet cable that is connected from your DSL or cable modem to your computer and plug it into the WAN port on the SOHO unit. The SOHO unit is now connected directly to the modem.
- 4 Plug the Ethernet cable supplied with your SOHO into any one of the four (numbered 1-4) Ethernet ports on the SOHO. Plug the other end into the Ethernet card installed in your computer. The SOHO unit will then be connected between your modem and computer.
- 5 Restore the power to your DSL or cable modem. Wait until the indicator lights of the modem have stopped flashing indicating that the modem is ready.

- 6 Attach the power cord to the SOHO and plug it into an outlet.
- 7 Restart your computer.
- 8 For information on the factory default configuration options, see “The Default Factory Settings” on page 22. For specialized configurations, see “Configuring Your External Network” on page 37, as well as, “Configuring Your Trusted Network” on page 47.

### **Cabling the SOHO for more than four computers**

While there are only four (numbered 1-4) Ethernet ports on the back of the SOHO, you can connect many more devices to your SOHO using network hubs.



The SOHO and SOHO | tc ship with a “10-seat” license. In other words, the SOHO allows up to ten computers on a network behind the SOHO to access the Internet. More than ten computers can

exist on the network and communicate with each other, but only the first ten which attempt to access the Internet will be allowed through the SOHO. If you would like to upgrade your SOHO to a twenty-five or fifty-seat user license, please visit:

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

- 1 Complete the "Pre-installation checklist" on page 27.
- 2 You will need these additional items:
  - One or more Ethernet hubs.
  - An Ethernet cable (with RJ-45 connectors) for each computer to connect to the SOHO.
  - An Ethernet cable to connect each hub to the SOHO.
- 3 Turn off your computer and unplug the power from the cable or DSL modem.
- 4 Unplug the Ethernet cable that is connected from your cable or DSL modem to your computer, and instead connect it from your modem to the WAN port on the SOHO.  
This creates a connection between the SOHO and the modem.
- 5 Plug an Ethernet cable into any of the four (numbered 1-4) Ethernet ports on the SOHO. Plug the other end into an Ethernet hub.
- 6 Using Ethernet cables, connect the hub uplink port to the Ethernet card installed in each of your computers.
- 7 Turn on the power to your cable or DSL modem. Wait until the lights stop flashing, indicating that the modem is ready.
- 8 Attach the power cord to the SOHO and plug it into an outlet.
- 9 Restart your computer.



# Setting Up Your SOHO Network

---

The configuration instructions in this chapter assume that you are using Windows 98/ME. If this is not the case, see your operating system user guide or help resources to locate the equivalent options and commands.

## Configuring Your External Network

---

When you configure the external network, you establish how the SOHO communicates with your Internet service provider (ISP). This configuration is very much dependent on how your ISP distributes network addresses—using DHCP or PPPoE.

### Network addressing

Each networked computer in the entire world must have an IP address to identify itself to other computers. The most common

method to distribute IP addresses is to use Dynamic Host Configuration Protocol (DHCP). When you connect your computer to the network, a DHCP server at your ISP automatically assigns it a network IP address. This eliminates the ISP from having to manually assign and manage IP addresses.

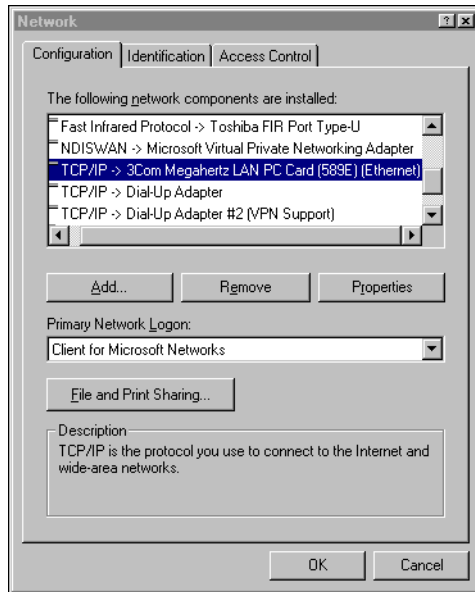
IP address assignments can be either dynamic or static. With dynamic, your ISP assigns your computer a new address every time you connect. When you power down, you release the address, and it may be reassigned. An IP address that is static, on the other hand, belongs to your computer at all times whether or not you are currently using it. No other computer anywhere on the network shares the same address.

A third way of assigning 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 enables them to use existing Dial-Up infrastructure such as billing, authentication, and security for DSL and cable modems.

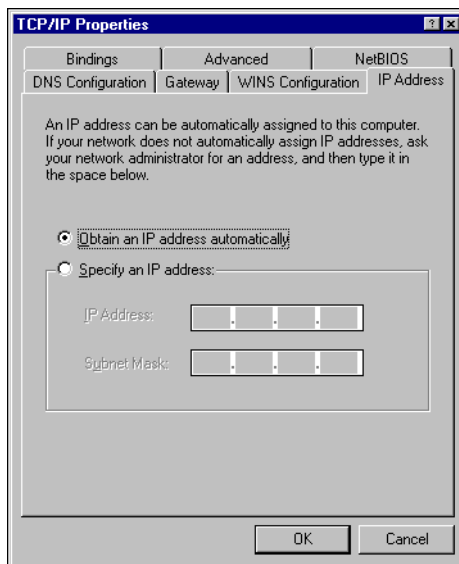
### **Determining whether your ISP uses dynamic or static addressing**

Most ISPs support both dynamic and static addressing. To determine if your connection to the Internet is dynamic or static:

- 1 Click **Start** ⇒ **Settings** ⇒ **Control Panel**.  
The Control Panel window appears.
- 2 Double-click the **Network** icon.  
The Network dialog box appears.



- 3 Scroll through the list of installed network components. Double-click the **TCP/IP** network component which is bound to your Ethernet card. Look for (Ethernet) in parentheses. The TCP/IP Properties dialog box appears.



- 4 If "Obtain an IP Address Automatically" is selected, your computer is configured for dynamic DHCP. If "Obtain an IP Address Automatically" is not checked, your computer is configured for static addressing.

### Configuring the SOHO External network for dynamic addressing

Out of the box, the SOHO is configured to obtain its external address information automatically, using DHCP. If your ISP supports this method, the SOHO will obtain all the necessary address information when it powers on and attempts to connect to the Internet. No further configuration of the SOHO is required. To complete the SOHO External Network configuration, see "Release and renew the IP configuration" on page 46.



## Configuring the SOHO 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. Instead of communicating directly to your computer, the ISP will now communicate first through the SOHO. To do this you must both modify the static settings on your personal computer as well as enter the information on the SOHO Configuration pages.

---

### NOTE

---

The SOHO supports a mini, onboard Web server which provides a Web page interface for configuring the unit. Therefore, the SOHO configuration pages are reached via your Web browser.

---

### On your computer:

- 1 Click **Start** ⇒ **Settings** ⇒ **Control Panel**.  
The Control Panel window appears.
- 2 Double-click the **Network** icon.  
The Network dialog box appears.
- 3 Double-click the **TCP/IP** network component which is bound to your Ethernet card. Look for **(Ethernet)** in parentheses.  
The Properties window appears with the addressing information already filled in.
- 4 Select the **Obtain an IP address automatically** option. Click **OK**.

---

### NOTE

---

The wording may differ slightly depending on the operating system. A similar option, however, is found on all platforms.

---

- 5 If prompted with “Do you want to enable DHCP?” click **Yes**.

- 6 Save the changes.
- 7 On most platforms, click **OK** until the Control Panel window closes.
- 8 Shut down and reboot the computer.

### **On the SOHO:**

- 1 Open your Web browser. 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 special configuration Web pages installed on the SOHO itself.
- 2 With your Web browser, go to the SOHO System Status page using the Trusted IP address of the SOHO.  
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.

The screenshot shows the WatchGuard SOHO Configuration interface. The left sidebar contains a navigation menu with categories: System Status, Network (External, Trusted, Routes, Network Statistics), Administration (System Security, VPN Manager Access, Update, Upgrade, View Configuration File), Firewall (Incoming, Outgoing, Custom Service, Blocked Sites, Firewall Options, DMZ), Logging (WSEP Logging, Syslog Logging, System Time), WebBlocker (Settings, Groups), and VPN (Remote Gateways, MUVN Clients, VPN Statistics). The main content area is titled 'SOHO Configuration' and 'External Network Configuration'. It features a 'Configuration Mode' dropdown menu set to 'Manual Configuration'. Below this are input fields for IP Address (206.253.208.100), Subnet Mask (255.255.255.0), Default Gateway (206.253.208.1), Primary DNS (206.253.208.254), Secondary DNS (206.253.208.253), and DNS Domain Suffix (inside.watchguard.com). At the bottom of the form are 'Submit' and 'Reset' buttons.

- 4 From the Configuration Mode drop list, select **Manual Configuration**.
- 5 Enter the TCP/IP settings you copied from the computer when you started the install process.
- 6 Click the **Submit** button.

To complete the SOHO External Network configuration, see “Release and renew the IP configuration” on page 46.

## Configuring the SOHO external network for PPPoE

While less common, PPPoE is another method for an ISP to assign 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. You will need your PPPoE login name and password.

To configure the SOHO 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 special configuration Web pages installed on the SOHO itself.

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

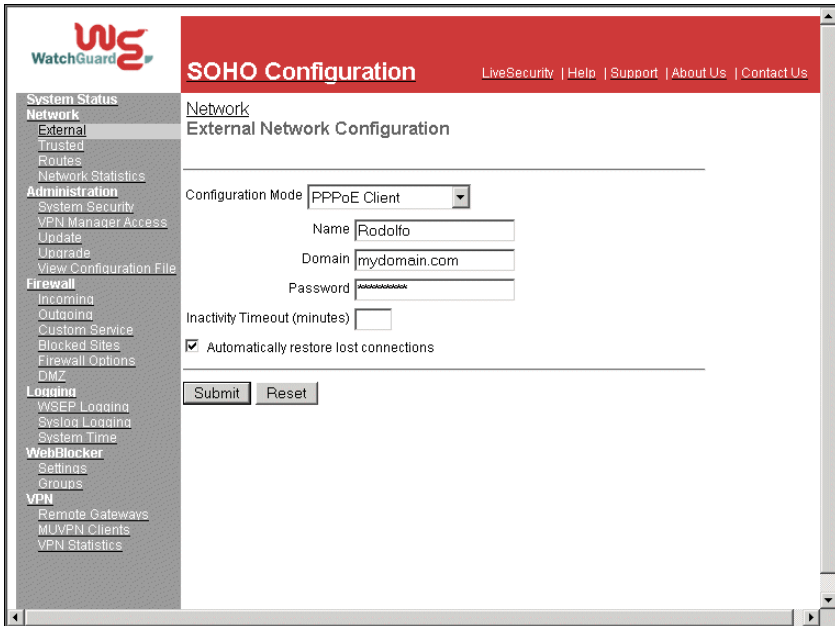
For example, if using the default IP address, go to: <http://192.168.111.1>

3 **From the navigation bar on the left side, select **Network => External**.**

The External Network Configuration page appears.

4 **From the Configuration Mode drop list, select **PPPoE Client**.**

The PPPoE Client configuration page appears.



- 5 Enter the PPPoE login name supplied by your ISP.
  - 6 Enter the PPPoE password supplied by your ISP
  - 7 **Click Automatically restore lost connections.**  
 This enables a constant flow of “heartbeat” traffic between the SOHO and the PPPoE server. In the event of routine packet loss, this option allows the SOHO to maintain the PPPoE connection. The SOHO may reboot to recover this connection if the heartbeat fails. This provides for a more consistent Internet connection but will be seen as continuous traffic by the ISP and regulated as such.
  - 8 **Click the Submit button.**  
 The configuration change is saved to the SOHO.
- To complete the SOHO External Network configuration, see “Release and renew the IP configuration” on page 46.

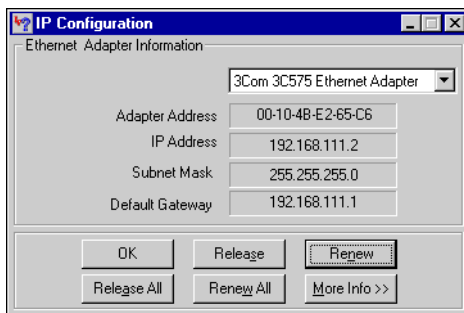
## Release and renew the IP configuration

Regardless of what type of addressing your computer used originally, it will now obtain this information from the SOHO using DHCP. To enable your computer to receive this information from the SOHO, you must force it to release and renew its IP configuration information.

From your computer desktop:

- 1 Click **Start** ⇒ **Programs** ⇒ **Command Prompt**.
- 2 At the C:\ prompt, type `wiipcfg`. Press **Enter**.  
The IP Configuration dialog box appears.
- 3 Verify that the information is displayed for "Ethernet Adapter," not for "PPP Adapter," which applies to a dial-up telephone modem.
- 4 Click the **Release** button. Then click the **Renew** button.

Your IP Configuration should look similar to the image below. The values in the IP Configuration dialog box were obtained from the SOHO itself. The IP Address, Subnet Mask and Default Gateway entries must be completed and have the values displayed for address sharing to work as in the example below.



## Configuring Your Trusted Network

---

Out of the box, the SOHO automatically uses DHCP to assign addresses to computers on your trusted network. In other words, every time you connect a computer to the SOHO, either directly or through a hub, it automatically attempts to obtain its addresses from the SOHO.

### Configure the Trusted network with static addresses

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

- 1 With your Web browser, go to the SOHO System Status page using the Trusted IP address of the SOHO.  
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 the WatchGuard SOHO Configuration web interface. The top navigation bar is red with the WatchGuard logo on the left and links for LiveSecurity, Help, Support, About Us, and Contact Us on the right. A left-hand menu lists various configuration categories: System Status, Network (External, Trusted, Routes, Network Statistics), Administration (System Security, VPN Manager Access, Update, Upgrade, View Configuration File), Firewall (Incoming, Outgoing, Custom Service, Blocked Sites, Firewall Options, DMZ), Logging (WSEP Logging, Syslog Logging, System Time), WebBlocker (Settings, Groups), and VPN (Remote Gateways, MUVPN Clients, VPN Statistics). The main content area is titled 'SOHO Configuration' and 'Network Trusted Network Configuration'. It contains two input fields: 'IP Address' with the value '10.0.0.1' and 'Subnet Mask' with the value '255.255.255.0'. Below these is a checkbox labeled 'Enable DHCP Server on Trusted Network' which is currently unchecked. A third input field is labeled 'First address for DHCP server'. At the bottom of the form are 'Submit' and 'Reset' buttons.

- 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 the **Submit** button.

### **Configure additional computers to the trusted network**

Up to four computers can be plugged directly into the four (numbered 1-4) Ethernet ports of the SOHO. A larger number of computers can be networked together by using one or more 10BaseT Ethernet hubs with RJ-45 connectors. The SOHO system will coexist with other systems over the same local area network



(LAN). You can also mix computers with different operating systems on your network and they will pass traffic through the SOHO to access the Internet.

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

- 1 Ensure that any 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 for more than four computers” on page 34. Restart the computer.
- 2 Set the computer to obtain its address dynamically.
- 3 Turn off and restart the computer.
- 4 Release and renew the IP configuration.  
see “Release and renew the IP configuration” on page 46. The computer will then obtain its TCP/IP settings dynamically from the SOHO unit.

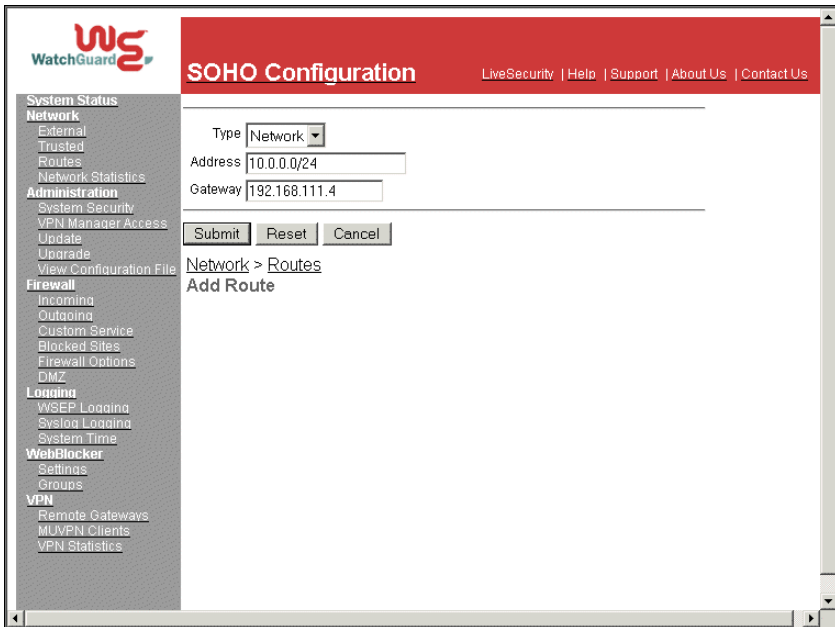
## Configuring Static Routes

---

The SOHO allows you to configure static routes in order to pass traffic to networks on separate segments. In other words, you can have additional networks connected to a router or switch behind the SOHO and the SOHO will route data packets to these networks.

Follow these instructions to configure static routes:

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



- 3 Click the **Add** button.
- 4 From the Type drop list, select either a **Host** or **Network**.
- 5 Enter the IP address and the Gateway of the route in the appropriate field.
- 6 Click the **Submit** button.

## View the Network Statistics

---

The SOHO has a configuration page which displays a variety of network statistics to assist you 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 SOHO System Status page using the Trusted IP address of the SOHO.  
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 displays the WatchGuard SOHO Configuration interface. The top navigation bar includes the WatchGuard logo and links for LiveSecurity, Help, Support, About Us, and Contact Us. A left-hand navigation menu lists various system settings, with 'Network Statistics' highlighted. The main content area shows the 'Network Statistics' page, which is divided into sections for IP, External Network, and Trusted Network. The IP section displays system uptime and network buffer statistics. The External Network section shows statistics for the USNet0 interface, including link encapsulation, hardware address, and packet counts for RX and TX. The Trusted Network section is partially visible at the bottom.

Section	Statistics
IP	IP: Up for 3 hours 22 minutes 48 seconds Network Buffers Allocated/Total (10/40) Memory Tot Sockets Allocated/Total (10/80) NAT Ports Avail (9) Tx: packets (45008) Rx: packets (55758) hdr Err(9404) delivered (2101) reassemble (76) forward (44199) reassemble OK (38) fragments OK (38) fragments created (76)
External Network	USNet0: Link encap:Ethernet HWaddr 00:90:7f:0f:52:ed inet RX packets:22238 errors:0 bcast:48829 disc:0 unk:5 TX packets:22373 errors:0 bcast:2 lnPci0: Tx: packets(22375) errs(49) collisions(0) stat(ff Rx: packets(71251) errs(0) flags(99) rindex (3) ti
Trusted Network	



# Your Administrative Options

---

The SOHO Administration page allows you to configure access to the unit, update the firmware from a non-Windows operating system, redeem any upgrade options you may have purchased, and see the SOHO configuration file in a text format.

## The System Security Page

---

The System Security configuration page allows you to create secure settings in order to protect the configuration of your SOHO. Setting a System Administrator Name and System Passphrase allows you to protect the SOHO by using a simple authentication method. Creating these settings is discussed in the section below.

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 in-

depth in the SOHO Remote Monument Guide located on our Web site:

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

## **Setting a System Administrator Name and System Passphrase**

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 System Administrator Name and System Passphrase are designed to protect the SOHO configuration from being altered by someone on your trusted network. In other words, when you have configured a SOHO System Administrator Name and System Passphrase, no one in your office will be able to change (deliberately or accidentally) your firewall settings without the System Administrator Name and System Passphrase.

---

### **CAUTION**

---

Take steps to ensure that you do not lose your System Administrator name and passphrase. Once you have enabled System Security protection, there is no other means of accessing your SOHO settings. Should you forget your name or passphrase, the only means of accessing the device requires reverting your SOHO to its factory settings; please see "Resetting a SOHO to the Factory Defaults" on page 23, you will then need to reconfigure your SOHO.

---

You should change your System Passphrase at least once a month to be secure. A passphrase should be a combination of letters, numbers, and symbols that do not spell out common words. It should contain at least one special character, number, and a mixture of upper and lower case letters.

Follow these steps to setup the SOHO System Passphrase:

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

The screenshot shows the WatchGuard SOHO Configuration interface. The left sidebar contains a navigation menu with categories like System Status, Network, Administration, Firewall, Loading, WebBlocker, and VPN. The main content area is titled 'SOHO Configuration' and 'Administration System Security'. It features several configuration fields: 'HTTP Server Port' set to 80, a checked 'Enable System Security' checkbox, 'System Administrator Name' (Padalund), 'System Passphrase' (masked), and 'Confirm System Passphrase' (masked). There is also an unchecked 'Enable SOHO Remote Management' checkbox, a 'Virtual IP Address' field (0.0.0.0), and dropdown menus for 'Authentication Algorithm' (MD5-HMAC) and 'Encryption Algorithm' (DES-CBC). 'Submit' and 'Reset' buttons are at the bottom.

- 3 Verify that the HTTP Server Port is set at 80.
- 4 Enable the checkbox labeled **Enable Password**.
- 5 Enter the System Administrator Name in the appropriate field.
- 6 Enter the System Passphrase in the appropriate field.

- 7 Enter the System Passphrase again to confirm it in the appropriate field.
- 8 Click the **Submit** button.

## Setting up VPN Manager Access

---

The SOHO can be configured to allow the WatchGuard VPN Manager software access in order to configure and manage Branch Office VPN tunnels from a remote location.

The VPN Manager software is purchased separately. 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 SOHO System Status page using the Trusted IP address of the SOHO.  
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** ⇒ **VPN Manager Access**.  
The VPN Manager Access page appears.



The screenshot shows the WatchGuard SOHO Configuration interface. The top navigation bar includes the WatchGuard logo, the title "SOHO Configuration", and links for LiveSecurity, Help, Support, About Us, and Contact Us. A left-hand navigation menu lists various configuration categories: System Status, Network (External, Trunks, Routes, Network Statistics), Administration (System Security, VPN Manager Access, Update, Upgrade, View Configuration File), Firewall (Incoming, Outgoing, Custom Service, Blocked Sites, Firewall Options, DMZ), Logging (WSEP Logging, Syslog Logging, System Time), WebBlocker (Settings, Groups), and VPN (Remote Gateways, MUVPN Clients, VPN Statistics). The main content area is titled "Administration" and "VPN Manager Access". It features a checked checkbox labeled "Enable VPN Manager Access". Below this are four password fields: "Status Passphrase", "Confirm Status Passphrase", "Configuration Passphrase", and "Confirm Configuration Passphrase". At the bottom of the form are "Submit" and "Reset" buttons.

- 3 Enable the checkbox labeled **Enable VPN Manager Access**.
- 4 Enter the Status Passphrase in the appropriate field.
- 5 Enter the Status Passphrase in the appropriate field again to confirm it.
- 6 Enter the Configuration Passphrase in the appropriate field.
- 7 Enter the Configuration Passphrase in the appropriate field again to confirm it.

---

### CAUTION

---

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

---

- 8 Click the **Submit** button.

## Update Your Configuration from a Non-Windows Platform

---

If you are managing your SOHO from a computer running a operating system platform 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 built for Windows only.

Follow these steps to perform this procedure:

- 1 With your Web browser, go to the SOHO System Status page using the Trusted IP address of the SOHO.  
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.
- 3 Read through the End-User License Agreement document, then enable the **I accept the above license agreement** checkbox at the bottom of the page.
- 4 Enter the location of the firmware files located on your computer in the appropriate field.
- 5 If you do not know the location of the firmware files, click the **Browse** button to browse your computer's directories and select them.
- 6 Click the **Update** button.

## Redeeming your SOHO upgrade certificates

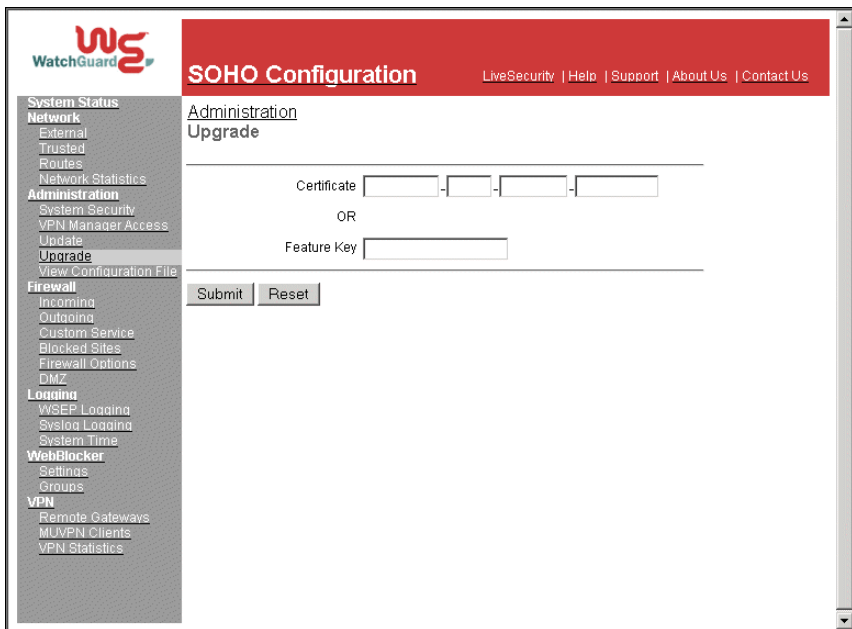
---

When you purchase a SOHO, 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 which enables

these software options is stored within the SOHO. Once you have purchased an upgrade option and redeemed it, the Feature key stored on your unit is modified to enable the software upgrade.

Follow these steps to redeem your upgrade certificate:

- 1 With your Web browser, go to the SOHO System Status page using the Trusted IP address of the SOHO.  
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** ⇒ **Upgrade**.  
The Upgrade page appears.



- 3 Enter the Certificate number in the appropriate field.
- 4 Click the **Submit** button.

## **Upgrade certificates**

### *Seat Licenses*

The SOHO can be upgraded to provide for more seats than are available with the base model (for example, the 25 seat license certificate). These certificates must be purchased separately.

### *IPSec Virtual Private Networking (VPN)*

The SOHO | tc comes with a VPN upgrade certificate, however you must first enable the VPN upgrade in order to configure virtual private networking. The SOHO does not come with the VPN upgrade certificate. It can be upgraded, but this certificate must be purchased separately.

### *WebBlocker*

The SOHO can be upgraded to provide a web filtering option. This certificate must be purchased separately.

### *MUVPN Clients*

The SOHO can be upgraded to allow single remote users to securely connect to it through an IPSec VPN and access network resources on the Trusted network. These certificates must be purchased separately.

### *LiveSecurity Service Subscription Renewals*

Subscriptions may be renewed for one or two years. You can purchase a renewal certificate from your reseller or buy it online. Log in to the LiveSecurity Service and click Subscription Renewals (even expired users can log in to renew their subscriptions) at:

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

Follow the instructions printed on the certificate to activate the renewal.

## View the Configuration File

---

From this configuration page, you can view your SOHO configuration file as it appears in text form.

Follow these steps to view the file:

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



# Configuring Your Firewall Settings

---

## Firewall settings

---

The WatchGuard SOHO enables you to customize what is allowed both incoming and outgoing through your firewall. With this feature, you can narrowly define what kind of communication is permitted between computers on the Internet and computers on your trusted network.

To facilitate configuring your SOHO, WatchGuard identifies several commonly used services. A service is the combination of protocol and port numbers associated with a specific application or communication type.

---

## Configuring Incoming and Outgoing Services

---

By default, the security stance of the SOHO is to deny unsolicited incoming packets to computers on the trusted network protected

by the SOHO firewall. You can, however, selectively open your network to certain types of Internet connectivity. For example, if you would like to set up a Web server behind the SOHO, you can 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.

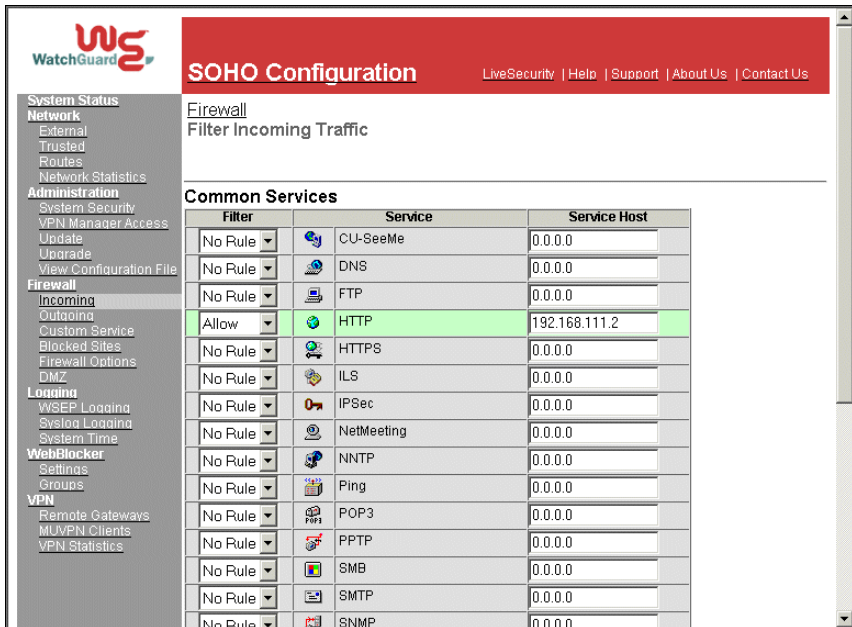
### **Pre-configured Services**

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 WatchGuard SOHO Configuration pages include several of the most common types.

Follow these steps to add a Incoming service:

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





- 2 Locate the pre-configured service you wish to define, 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 will apply.  
In our example, 192.168.111.2.
- 4 Click the **Submit** button.

## Creating a Custom Service

In addition to the pre-configured services provided by the WatchGuard SOHO Configuration interface, you can create a

custom service using either a TCP port, UDP port or specifying an IP protocol. You can also create a custom service allowing *any* form of protocol over *any* port incoming from an external address to a trusted host or outgoing from a trusted host to an external address.

### TCP and UDP Ports

Follow these steps to create a custom service for either TCP or UDP ports:

- 1 With your Web browser, go to the SOHO System Status page using the Trusted IP address of the SOHO.  
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 either **TCP Port** or **UDP Port** from the drop list.  
The Custom Service page refreshes.
- 4 Define a name for the service in the appropriate field.

### IP Protocols

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.

Follow these steps to create a custom service for an IP protocol:

- 1 With your Web browser, go to the SOHO System Status page using the Trusted IP address of the SOHO.  
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 either **TCP Port**, **UDP Port** or **Protocol** from the drop list.

The Custom Service page refreshes.

- 4 Define a name for the service in the appropriate field.
- 5 Enter the protocol number to allow in the Protocol field.

Now that you have created a custom service, you will 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 configuration page refreshes.
- 8 Enter either a single host IP address, a network IP address, or a the start and end of a range of host IP addresses for this custom service in the appropriate fields.
- 9 Click the **Add** button.  
Repeat the last three steps until all the appropriate address information for this custom service appears in the appropriate fields.
- 10 Click the **Submit** button.

## Blocking External Sites

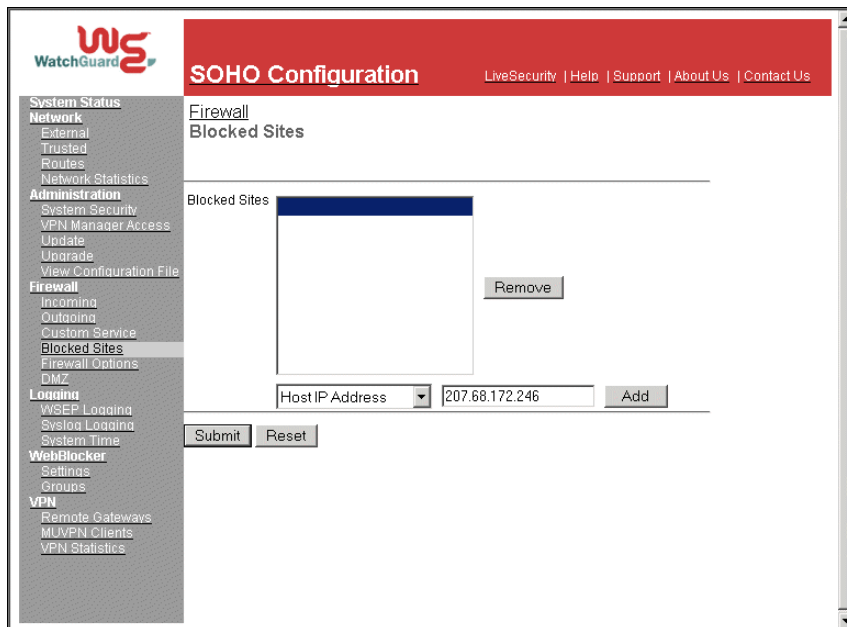
---

By default, the security stance of the SOHO is to deny all incoming packets from the Internet to computers on the trusted network protected by the SOHO firewall. However, if a user initiates contact with an external site, the return traffic will be allowed through the firewall. You can selectively close your network to certain 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.



- 2 Select either Host IP Address, Network IP Address, or Host Range from the drop list.  
The configuration page refreshes.
- 3 Enter either a single host IP address, a network IP address, or a 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 the **Add** button.  
The addressing appears in the Blocked Sites field.

- 5 Click the **Submit** button.

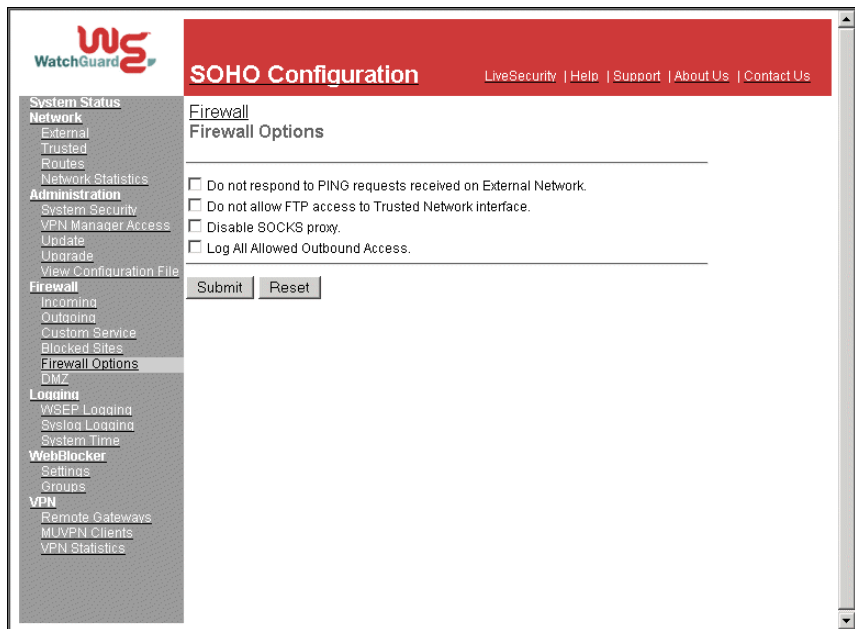
## Firewall Options

---

The SOHO firewall feature includes a few rule settings which are less specific than the service settings discussed previously and can be 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 SOHO System Status page using the Trusted IP address of the SOHO.  
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.



### **Ping requests received on the External Network**

You can configure the SOHO to deny all ping packets which it may receive on the external interface.

- 1 Enable the checkbox labeled **Do not respond to PING requests received on External Network**.
- 2 Click the **Submit** button.

## Denying FTP access to the Trusted Network interface

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

- 1 Enable the checkbox labeled **Do not allow FTP access to Trusted Network**.
- 2 Click the **Submit** button.

---

### CAUTION

---

When performing an update of the system firmware, this option must be disabled or the procedure will fail and the unit becomes unrecoverable and must be reset to the factory defaults. If this inadvertently occurs, please see "Resetting a SOHO to the Factory Defaults" on page 23.

---

## SOCKS implementation for the SOHO

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 SOCKS-aware) 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, the application must be configured with the SOCKS server information.

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

The SOHO SOCKS feature has the following characteristics and limitations:

- SOHO supports SOCKS version 5 only.
- It is a limited version of SOCKS and does not support authentication, nor does it support Domain Name System (DNS) resolution.

---

### CAUTION

---

Configure the particular application so that it will *not* attempt to make DNS look-ups with SOCKS. However, some applications use only DNS through SOCKS and therefore will not function properly with the SOHO.

---

- Compatible SOCKS-aware applications that can be used through the SOHO include ICQ, IRC, and AOL Messenger.
- When you open a SOCKS application, it opens a “hole” in the SOHO firewall that is 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” on page 73.

### Configure your SOCKS application

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

- If you can choose different services or versions of SOCKS, choose SOCKS version 5.
- Select port 1080 for the application



- For the SOCKS proxy, enter the URL or IP address of the SOHO trusted network. The default IP address is 192.168.111.0.

### **Disabling SOCKS on the SOHO**

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

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

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

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

### **Logging all allowed outbound traffic**

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

---

#### **NOTE**

As this option will record an extensive amount of log entries, WatchGuard recommends that it only be enabled for diagnostic purposes.

---

Follow these steps:

- 1 Enable the checkbox labeled **Log All Allowed Outbound Access**.
- 2 Click the **Submit** button.

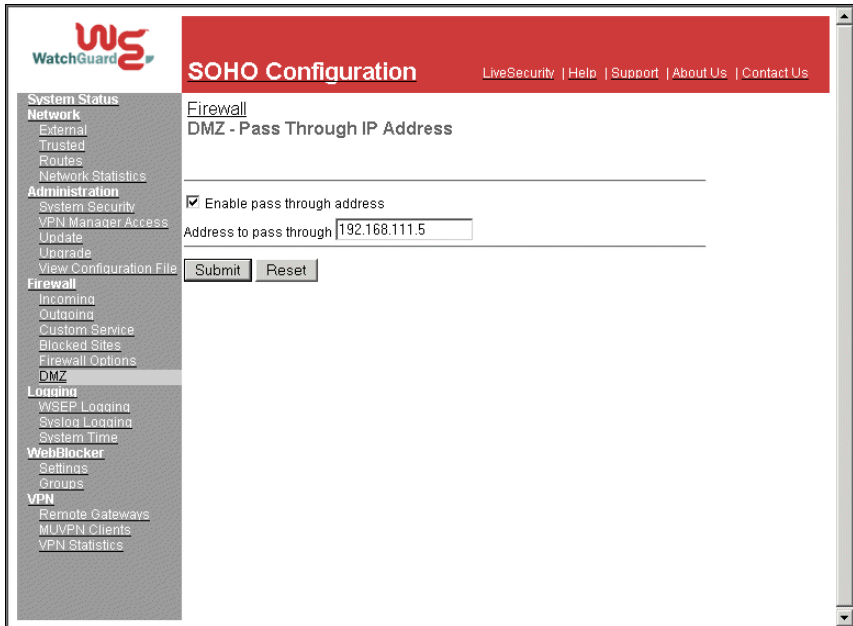
## Creating a virtual DMZ

---

The SOHO can be configured to allow traffic to be passed through to a dedicated machine that has been separated from the rest of the Trusted Network.

Follow these steps to configure DMZ pass through:

- 1 With your Web browser, go to the SOHO System Status page using the Trusted IP address of the SOHO.  
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** ⇒ **DMZ**.  
The DMZ page appears.



- 3 Enable the checkbox labeled **Enable pass through address**.
- 4 Enter the IP address to the pass through machine in the appropriate field.
- 5 Click the **Submit** button.



# What is Logging?

---

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

Logging is intended to record the kinds of activities that can indicate security concerns—most importantly denied packets. Certain patterns of denied packets can indicate the type of attack that is being attempted.

## Viewing SOHO log messages

---

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

The log messages may include time synchronizations between the SOHO and the WatchGuard Key Server, discarded packets for a packet handling violation, duplicate messages, time-outs for attempting to open the WatchGuard Feature Key Server, or return error messages.

Follow these steps to view these log messages:

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

## Setting a WatchGuard Security Event Processor log host

---

Setting a remote log host causes log messages to be transmitted to a WatchGuard Security Event Processor server (participating in a WatchGuard Firebox System™ solution) preconfigured to accept logs from your SOHO. It has the advantages of saving local resources for other less memory-intensive tasks and puts the log host at the WatchGuard Firebox System site where customer support can examine logs at your request to troubleshoot security problems.

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

The screenshot shows the WatchGuard SOHO Configuration web interface. The top navigation bar includes the WatchGuard logo and links for LiveSecurity, Help, Support, About Us, and Contact Us. A left-hand navigation menu lists various configuration categories such as System Status, Network, Administration, Firewall, Logging, WebBlocker, and VPN. The main content area is titled "SOHO Configuration" and "Logging". Under the "Logging" section, there is a heading "WatchGuard Security Event Processor Logging". A checkbox labeled "Enable WatchGuard Security Event Processor Logging" is checked. Below this, there are three input fields: "Log Host IP Address" with the value "206.253.208.100", "Log Encryption Key" with a masked password, and "Confirm Key" with the same masked password. At the bottom of the form are "Submit" and "Reset" buttons.

- 3 Enable the checkbox labeled **Enable WatchGuard Security Event Processor Logging**.
- 4 Enter the IP address of the WSEP server that will be your Log Host in the appropriate field.  
In our example, 206.253.208.100.
- 5 In the **Log Encryption Key** field, enter a passphrase that will serve as a password to gain access to the log server.
- 6 Enter the Log Encryption Key passphrase in the appropriate field again to confirm it.
- 7 Click the **Submit** button.

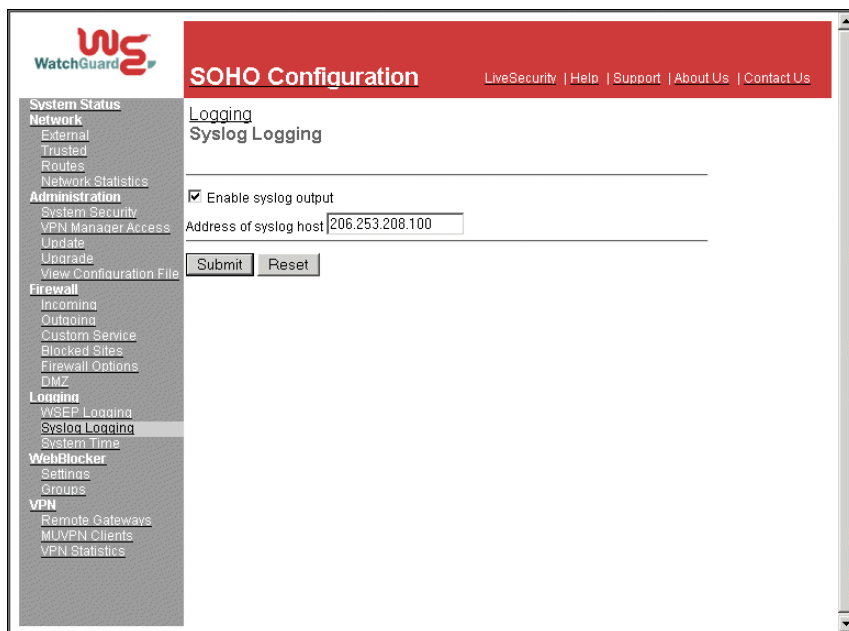
## Setting a Syslog Host

---

The SOHO can also be configured to transmit log entries to a Syslog host.

Follow these steps to setup a Syslog Host:

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



- 3 Enable the checkbox labeled **Enable syslog output**.



- 4 Enter the IP address of the Syslog server in the appropriate field.  
In our example, 206.253.208.100.
- 5 Click the **Submit** button.

## Setting the System Time

The SOHO stamps each log entry with the time that the event occurred. By default, the SOHO is set to record event times in seconds beginning from the last time the unit was rebooted.

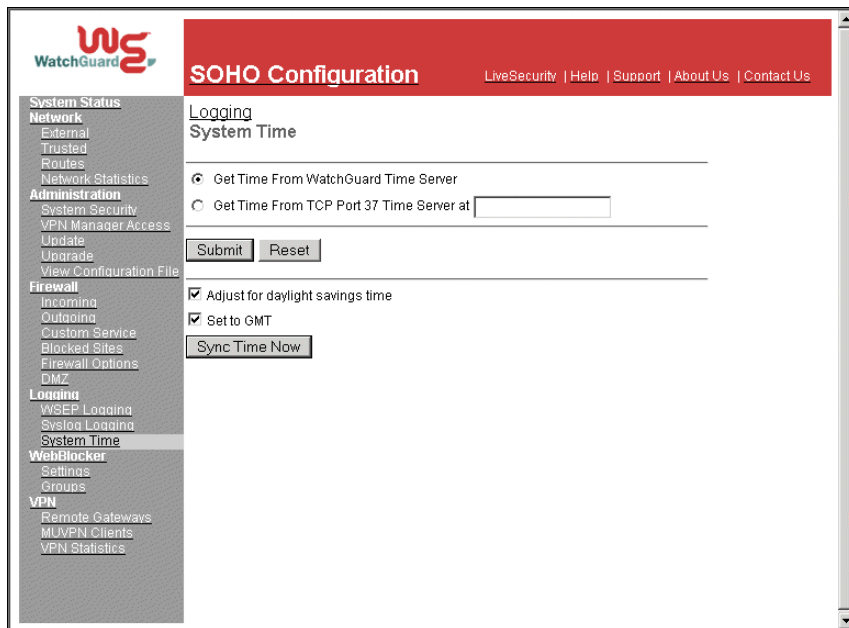
Event Log		
Time	Category	Message
26899 seconds	MONITOR	Administrator access allowed from 192.168.111.2
	IP	entry duplicated 1 times
26552 seconds	IP	ICMP type (0) code (0) received from 192.168.130.3

For example, in the image above, the top log entry indicates that the Administrator was allowed access to the unit 26899 seconds since the last power cycle.

The log entry time stamp can be configured to display the time of day by setting the System Time.

Follow these steps to set the System Time:

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



If you have decided to use the WatchGuard Time Server:

- 3 Enable the option labeled **Get Time From WatchGuard Time Server**.

Or, if you have decided to use a TCP Port 37 Time Server:

- 4 Enable the option labeled **Get Time From TCP Port 37 Time Server at**.
- 5 Enter the IP address of the time server in the appropriate field.
- 6 Click the **Submit** button.

If you want to have your log messages adjusted for daylight savings time or set to Greenwich Mean Time (GMT):

- Enable the checkbox labeled **Adjust for daylight savings time**.

- Enable the checkbox labeled **Set to GMT**.

If you want to have your log messages sync with your computer:

- Click the **Sync Time Now** button.



# WatchGuard SOHO WebBlocker

---

WatchGuard SOHO WebBlocker is an optional feature of the WatchGuard SOHO and SOHO | tc 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, the CyberNOT list, a service of CyberPatrol, owned and maintained by SurfControl. The WebBlocker database contains many thousands of IP addresses and directories. These addresses are divided into categories based on content such as Drug Culture, Intolerance, or Sexual Acts.

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

Once you have purchased and enabled WebBlocker, every time a user on your trusted network attempts to reach an Internet Web

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

### **Web site not in WebBlocker database**

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

### **Web site in WebBlocker database**

If the site is in the WatchGuard WebBlocker database, the SOHO checks whether or not you have chosen 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*

This feature allows you to create a group and prescribe a given web browsing profile by selecting the WebBlocker categories you want to prevent members of this group from browsing over the internet.

### *Users*

This feature allows you to create an individual user account, with a unique username and password, and restrict their web browsing by assigning them to a given Group.

## **Bypassing the SOHO WebBlocker**

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

The SOHO WebBlocker configuration page includes a Full Access Password field. You can configure this password and give it to only those members of your trusted network who should be able 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 can browse any site on the Internet until either the Password Expiration duration passes or the individual closes the browser.

## **Purchasing and enabling SOHO WebBlocker**

---

To use WatchGuard SOHO WebBlocker, you must first purchase and enable the WebBlocker upgrade certificate. For information on redeeming upgrade certificates, please see, "Redeeming your SOHO upgrade certificates" on page 58.

## Configuring the SOHO WebBlocker

---

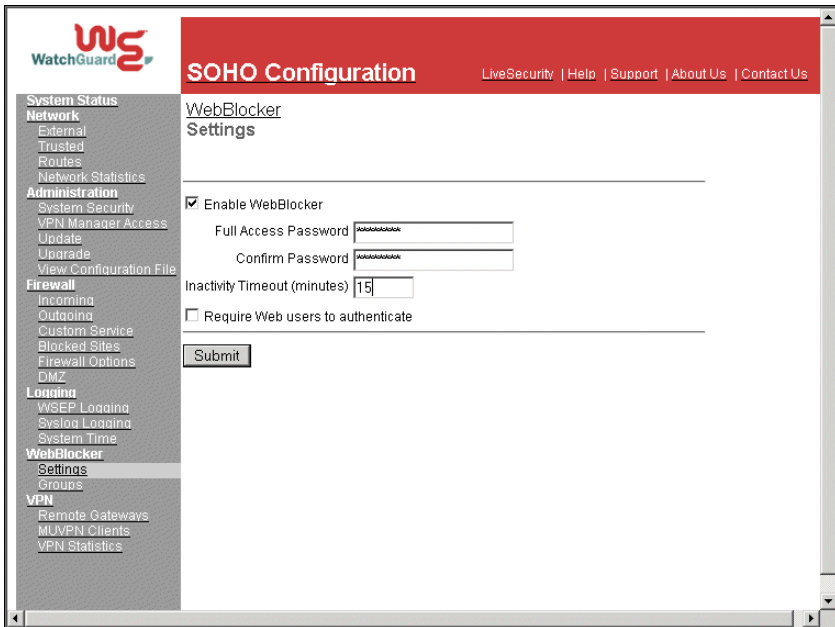
Use the WatchGuard SOHO Configuration pages to enable WebBlocker, create a full access password for bypassing WebBlocker, define an Inactivity Timeout which sets the duration that the full access password is valid, define the categories you want to block, and configure WebBlocker Groups and Users.

### Enable WebBlocker

Follow the instructions below to enable WebBlocker, create a Full Access Password, define the inactivity timeout value, 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 Configuration Settings page using the Trusted IP address of the SOHO.  
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.



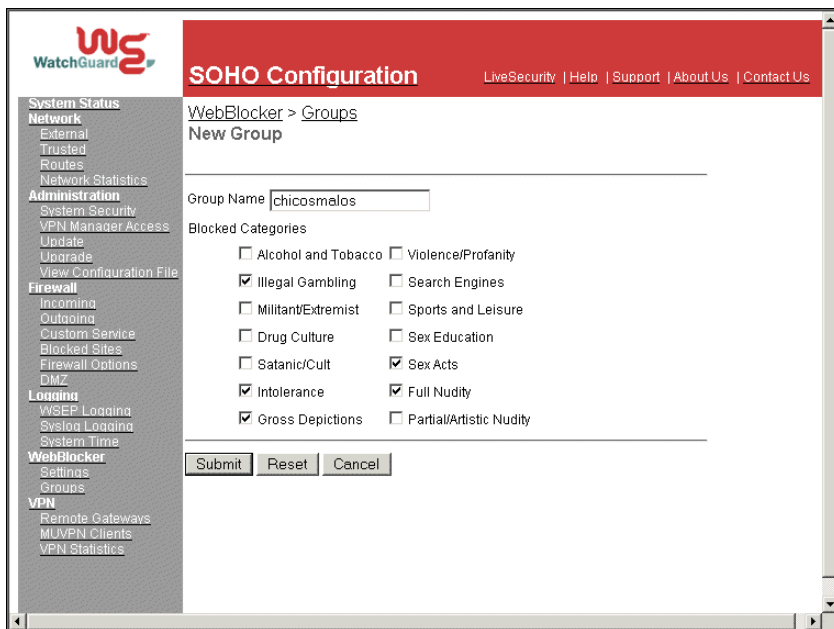


- 3 Enable the checkbox labeled **Enable WebBlocking**.
- 4 Enter the full access password.  
The full access password allows a user a to bypasses otherwise blocked sites.
- 5 Enter the Inactivity Timeout in minutes.  
Setting the inactivity timeout at, for example, 15 minutes, ensures that unattended Web browsers will be disconnected after sitting idle for 15 minutes.
- 6 If you intend to use WebBlocker Groups and Users, enable the **Require Web users to authenticate** checkbox.
- 7 Click the **Submit** button to register your changes.

## Create WebBlocker Groups and Users

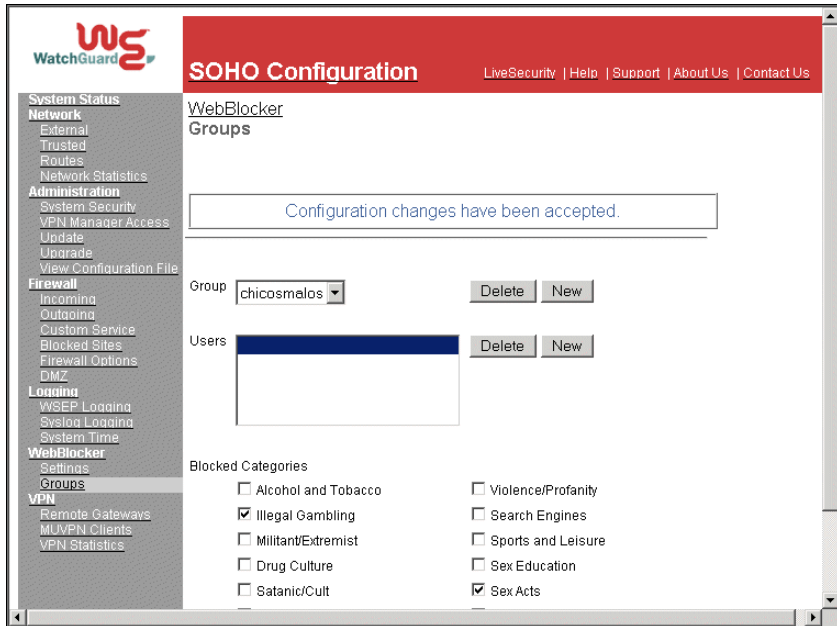
Follow the instructions below to create WebBlocker Groups. If you wish to use a global policy for all users, instead of creating separate group policies, ignore this section and follow the instructions to enable WebBlocker without selecting a Group.

- 1 With your Web browser, go to the SOHO Configuration Settings page using the Trusted IP address of the SOHO. 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.
- 3 Click the **New** button to create a group name and profile. In our example we have created the group "chicosmalos".



4 Click the **Submit** button.

A new Groups page appears indicating the configuration changes have been accepted and providing access to creating users.



5 To the right of the “Users” field, click the **New** button.

The New User page appears.

The screenshot shows the WatchGuard SOHO Configuration web interface. The top navigation bar includes the WatchGuard logo, the title 'SOHO Configuration', and links for LiveSecurity, Help, Support, About Us, and Contact Us. A left-hand navigation menu lists various configuration categories: System Status, Network (External, TruStes, Routes, Network Statistics), Administration (System Security, VPN Manager Access, Update, Upgrade, View Configuration File), Firewall (Incoming, Outgoing, Custom Service, Blocked Sites, Firewall Options, DMZ), Logging (WSEP Logging, Syslog Logging, System Time), WebBlocker (Settings, Groups), and VPN (Remote Gateways, MUVN Clients, VPN Statistics). The main content area is titled 'WebBlocker > Groups' and 'New User'. It contains a form with the following fields: 'User name' (text input with 'Rodolfo'), 'Passphrase' (password input with masked characters), 'Confirm Passphrase' (password input with masked characters), and 'Group' (dropdown menu with 'chicosmalos' selected). Below the form are three buttons: 'Submit', 'Reset', and 'Cancel'.

- 6 Enter a unique User name and Passphrase (remember to confirm the Passphrase). Use the Group drop down list to assign the new user to a given group.  
In our example, we have assigned the User "rodolfo" to the Group "chicosmalos" created previously.
- 7 Click the **Submit** button.

---

### NOTE

You can delete Users or Groups at any time by selecting them and clicking the **Delete** button.

---

## WebBlocker categories

---

WebBlocker relies on a URL database, the CyberNOT list, a service of CyberPatrol. The WebBlocker database contains many thousands of IP addresses and directories. These addresses are divided into categories based on content such as Drug Culture, Intolerance, or Sexual Acts. CyberPatrol constantly searches the Internet to update the list of blocked sites. The WebBlocker database contains the following 14 categories.

---

### NOTE

---

In all of the categories 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. Includes substances 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 devices, 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.

## Searching for blocked sites

---

To verify whether WebBlocker is blocking a site as part of a category block, visit the Search/Submit form on the Cyber Patrol Web site.

- 1 Using your Web browser, go to:  
<http://www.cyberpatrol.com/cyberNOT/default.htm>
- 2 Scroll down to display the Cyber Patrol CyberNOT® Search Engine.
- 3 Type the URL of the site to check.
- 4 **Click Check if the URL is on the CyberNOT List.**  
The search engine results notify you whether or not the site is on the CyberNOT list. Use this site also to suggest a new site for both the CyberNOT and CyberYES list, as well as to request a site review.



# Configuring Virtual Private Networking

---

This chapter describes an optional feature of the WatchGuard SOHO: Virtual Private Networking (VPN) with IPsec.

The following WatchGuard SOHO products support IPsec tunnels:

- WatchGuard SOHO with VPN option enabled
- WatchGuard SOHO | tc

## Why create a virtual private network?

Virtual Private Networking (VPN) tunnels enable you to and 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, un-encrypted 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 will need

---

- One WatchGuard SOHO with VPN and an IPSec-compliant device.

---

### NOTE

---

While you can create a SOHO to SOHO VPN, you can also create a VPN with a WatchGuard Firebox or other IPSec-compliant devices.

---

- The following information from your Internet service provider for both devices:
  - Static IP address
  - Default gateway address
  - Primary domain name service (DNS) IP address
  - If available, a secondary DNS address
  - Domain name
- Network addresses and subnet mask for networks. By default, the Trusted, network address of the SOHO 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 devices 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 straight. WatchGuard recommends making a table of IP addresses such as the one outlined below.

**IP Address Table (example):**

<b>Item</b>	<b>Description</b>	<b>Assigned By</b>
External IP Address	The IP address that identifies the SOHO to the Internet.  <b>Site A:</b> 207.168.55.2 <b>Site B:</b> 68.130.44.15	ISP
External Subnet Mask	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.  <b>Site A:</b> 255.255.255.0 <b>Site B:</b> 255.255.255.0	ISP
Local Network Address	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: 10.0.0.0 — 255.0.0.0 172.16.0.0 — 255.240.0.0 192.168.0.0/16 — 255.255.0.0  <b>Site A:</b> 255.255.255.0 <b>Site B:</b> 255.255.255.0	You
Shared Secret	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"  <b>Site A:</b> OurLittleSecret <b>Site B:</b> OurLittleSecret	You
Encryption Method	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 therefore much more secure. It is also slower. Either 3DES or DES may be selected as long as both sides use the same method.  <b>Site A:</b> 3DES <b>Site B:</b> 3DES	You
Authentication	Both sides must use the same method.  <b>Site A:</b> MD5 <b>Site B:</b> MD5	You

## Obtaining the VPN upgrade

If you purchased a WatchGuard SOHO and would like to purchase the VPN upgrade from a reseller or e-tailer, open your Web browser to:

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

## Enabling the VPN upgrade

Whether you purchased a VPN upgrade separately or purchased the SOHO ltc (which comes with option enabled) you must first redeem the VPN upgrade before configuring virtual private networking. Enabling the VPN upgrade requires:

- An installed SOHO
- Internet connectivity
- A VPN upgrade certificate license

## Step-by-step instructions for configuring a SOHO VPN tunnel

---

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

<http://www.watchguard.com/support/interopvpn.asp>

## Special considerations

Consider the following before configuring your WatchGuard SOHO VPN network:

- You can connect only two devices together: a WatchGuard SOHO and either another SOHO or another IPSec-compliant

device. To set up multiple VPN tunnels, you will need to have at least one WatchGuard Firebox configured with the WatchGuard VPN Manager.

- Each device must be able to send messages to the other. If either device has a dynamically assigned Internet (IP) address (see “Network addressing” on page 37 for an explanation of dynamic IP addresses), it will not be able to find its remote counterpart.
- Both devices must be set to use the same encryption method. The two choices are DES or 3DES. When connecting two 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 is not a limitation of the SOHO device.

## **Frequently asked questions**

---

### **Why do I need a static external address?**

To create a VPN connection, one SOHO must be able to find its partner device. If the addresses were allowed to change, the SOHO could not find its remote computer.

### **How do I get a static external IP address?**

Contact your ISP. Some systems, like many cable modem systems, use dynamically assigned addresses to simplify basic installations. Some providers may also use this feature to discourage users from creating Web servers. These providers usually offer a static IP address option.

## **How do I connect three or four offices together?**

To connect more than two offices together, WatchGuard recommends designating one office the center of a “star” network configuration and upgrading it to a WatchGuard Firebox. You can then manage multiple tunnels to SOHOs or other IPSec compliant devices from the central Firebox.

## **How do I troubleshoot the connection?**

If you can ping the remote SOHO 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.

## **OK, why is ping not working?**

If you cannot ping the local network address of the remote SOHO, take the following steps to classify the problem:

- 1 Ping the external address of the remote SOHO.  
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 can access the internet. If you are still having trouble, contact your ISP.
- 2 Once you can ping the external address of each SOHO, try pinging the local address.  
From Site A, ping 192.168.112.1. If the tunnel is up, you should get a reply from the remote SOHO. If not, re-check the Local Settings page. Make sure that the local DHCP addresses ranges do not overlap. For example, IP addresses on either side of the tunnel must not be the same.

## **How do I obtain a VPN upgrade certificate?**

Upgrade certificates come inside the box when you buy a WatchGuard SOHO ltc. They can also be purchased 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 can be found online at:

[http://www.watchguard.com/AdvancedFaqs/sointerop\\_main.asp](http://www.watchguard.com/AdvancedFaqs/sointerop_main.asp)

## MUVPN Clients

---

The SOHO can be upgraded to use the MUVPN clients option. This feature allows single remote users to securely connect to the SOHO through an IPSec VPN tunnel and access network resources on the Trusted network. Complete documentation on configuring your SOHO once this upgrade option has been purchased and redeemed can be found online at:

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

## View the VPN Statistics

---

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





---

## Troubleshooting

---

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

### General

#### How do I reboot my SOHO?

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

---

**NOTE**

---

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

---

### **What do the ON and MODE lights signify on the SOHO?**

When the ON light is illuminated, the SOHO has power. When the MODE light is illuminated, the SOHO is operational.

If the ON light is *blinking* it is indicative of a couple of concerns:

- If the MODE light is off than the unit is running through it's boot process and the ON light will cease blinking when the process is complete.
- If the MODE light is illuminated then the unit is running from it's backup flash memory. You should be able to connect to the unit from a computer on one of the four (numbered 1-4) Ethernet ports and reload the configuration.

If the MODE light is *blinking* it is indicative of a couple of concerns:

- The unit required a DHCP assigned IP address for the External interface (WAN) port but did not receive it.
- The External interface (WAN port) is not connected to another device, the physical connection is faulty, or the other device is not operating properly.

### **How do I register my SOHO?**

Registering your WatchGuard SOHO ensures that you receive all LiveSecurity alerts and software updates as soon as they are

available. The first year of service is free with purchase of the SOHO. To register your SOHO:

- 1 With your Web browser, go to the SOHO System Status page using the Trusted IP address of the SOHO.  
For example, if using the default IP address, go to: <http://192.168.111.1>
- 2 Click on **LiveSecurity** in the top header and follow the instructions provided.
- 3 Click on the **Register your SOHO** link, beneath the “New Subscribers Activate here header”.
- 4 Enter your information and then click **Save Profile**.

### **I set a password on my unit, but I forgot it. Can you help?**

If you forgot your password, you must reset the SOHO to its factory default. Please see the section titled, “Resetting a SOHO to the Factory Defaults” on page 23.

### **How does the seat limitation on the SOHO work?**

The default user license on the SOHO is 10. The first 10 computers on the network behind the SOHO to access the Internet are allowed through the SOHO. To clear the list of these first 10 computers you will need to reboot the SOHO.

### **What is a SOHO feature key?**

The feature key is an encrypted mask that tells the SOHO which features are enabled. It is stored in memory on the SOHO.

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

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

DSL router, the NAT feature of the DSL router should be set for bridge-only mode.

### **How do I install a SOHO using a Macintosh?**

The process is essentially identical to installing on any other platform. Use the Installation chapter within this Guide. The one unique element for Macintosh users, determining your TCP/IP settings, can be found on page 29.

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

There are twelve lights on the front of the SOHO grouped in pairs. The Link light labeled WAN tells you if your SOHO is connected to your modem. If this light is not illuminated, the SOHO is not connected to your modem. Check to make sure that both sides of the cable are connected and that your Internet connection is not down. The Link lights numbered 1 through 4 correspond to the four number Ethernet ports for the Trusted network. They tell you if the SOHO is connected to a computer or hub. If the lights are not illuminated, the SOHO 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 is on, but something may be wrong with the connection from the SOHO 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. If these are illuminated than your ISP may be temporarily down--you will need to call your ISP.

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

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

- 1 With your Web browser, go to the SOHO Configuration Settings page using the Trusted IP address of the SOHO.  
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 will see the External Network header on the right side. The MAC address is listed there.

## Configuration

### Where are the SOHO settings stored?

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

### How do I change to a DHCP trusted IP address?

- 1 Make sure your computer is set up to use DHCP dynamic addressing please see, "Release and renew the IP configuration" on page 46.
- 1 With your Web browser, go to the SOHO System Status page using the Trusted IP address of the SOHO.  
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 Enable the checkbox labeled **Enable DHCP Server** and then click the **Submit** button.

## 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 SOHO System Status page using the Trusted IP address of the SOHO.  
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 the checkbox labeled **Enable DHCP Server** and then click the **Submit** button.
- 4 Enter the information in the appropriate fields. Click the **Submit** button.

## How do I set up and disable Webblocker?

- 1 With your Web browser, go to the SOHO System Status page using the Trusted IP address of the SOHO.  
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 Enable the checkbox labeled **Enable WebBlocker**. Enter a Full Access password, and an Inactivity Timeout (in minutes).

To disable Web blocking, disable the checkbox labeled **Enable WebBlocker**.

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

- 1 With your Web browser, go to the SOHO System Status page using the Trusted IP address of the SOHO.  
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 the **Submit** button.

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

You will need the IP address of the computer that will be 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 SOHO System Status page using the Trusted IP address of the SOHO.  
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 either **TCP Port**, **UDP Port** or **Protocol** from the drop list.  
The Custom Service page refreshes.
- 4 Define a name for the service in the appropriate field.
- 5 Enter the protocol number to allow in the Protocol field.
- 6 Click the **Submit** button.
- 7 From the navigation bar on the left side, select **Firewall** ⇒ **Incoming**.  
The Firewall Incoming Traffic page appears.
- 8 Towards 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 will be allowed.
- 10 Click the **Submit** button.

## VPN Management

Before setting up a VPN, you must have the following:

- Two properly configured and working SOHOs or one SOHO and one Firebox with the latest version of firmware. Each SOHO must have the VPN option enabled.
- The static external IP address, the network address, and the subnet masks of both devices. (The base trusted IP address of each SOHO 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 for VPN Manager Access?**

This requires the add-on product, WatchGuard VPN Manager software, which is purchased separately. 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, see the VPN Manager Guide.

### **How do I set up VPN between two SOHOs?**

For detailed information on how to configure a VPN tunnel between two SOHO devices, download the SOHO to SOHO IPsec VPN Tunnel configuration instructions:

- 1 Using your Web browser, go to:  
<http://www.watchguard.com/support>
- 2 Login to the LiveSecurity site.
- 3 Click **Knowledge Base** on the left of the page.
- 4 Click the **In-Depth FAQ** link.
- 5 Under the Virtual Private Networking (VPN) header, click the **SOHO VPN Interoperability** link.
- 6 Click the **Configuring a WatchGuard SOHO to SOHO IPsec Tunnel** link.
- 7 Follow the instructions to configure your VPN tunnel.

## Contacting Technical support

---

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

## Online Documenting 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/faqs/>

## Special Notices

---

- At the time of publication of this document, the online Help System has not been posted on the WatchGuard Web site. Therefore, clicking on the Help link at the top of the System Status page will redirect you to the WatchGuard Product Documentation page where you can find links to our knowledge base.

---

## B

- blocked sites
  - in WebBlocker 96
- Browser
  - Netscape 4.0
    - disabling HTTP proxy 31
- Browsers, supported 28

## C

- Cables, required 27
- Cabling, new SOHO 32
- Categories, WebBlocker 93
- certification, FCC 4
- Checklist, pre-installation 27
- Configure
  - PPPoE client 43
- Copyright Information 12
- Custom incoming services, creating 65
- Cyber Patrol, copyright information 12

## D

- Database
  - WebBlocker 85
- Default gateway 98
- DNS service
  - primary IP address 98
  - secondary IP address 98
- Domain name 98

## E

- Encryption, SOHO 101

## F

- FCC certification 4
- Frequently asked questions 99

---

## H

HTTP proxy  
  disabling 30

## I

ICQ, enable with SOCKS 71  
ICQ, IRC, AOL Messenger 72  
Incoming service  
  creating custom 65  
Information  
  copyright 12  
  patent 12  
Installation  
  cabling the SOHO 32  
  manual 28  
  pre-installation checklist 27  
Introduction 3  
  information & Internet 63  
  IP address 20  
  port number 20  
  protocol 20  
  services 21  
IP address 20  
  reason for static 101  
  static, obtaining 98  
IP configuration, releasing and renewing 46

## L

LED, troubleshooting 105  
Link LED  
  troubleshooting 105  
Linux, setting TCP/IP 29  
LiveSecurity  
  User ID 18  
Log host  
  setting remote 78

---

## M

Macintosh, setting TCP/IP 29  
Manual installation 28  
Masquerading 21

## N

Network  
    private network default factory settings 22  
Network Address Translation 21

## P

Part number, SOHO 12  
Password  
    saving 18  
Patent Information 12  
Ping 102  
Port number, introduction 20  
PPPoE, configuring client 43  
Pre-configured service,  
    adding 64  
Pre-installation, checklist 27  
Private network  
    setting default factory settings 22  
Protocol, introduction 20  
Proxy, disabling HTTP 30

## R

Releasing IP configuration 46  
Remote Log Host, setting 78  
Renewing IP configuration 46

## S

Serial number, saving 18  
Services

---

- adding pre-configured 64
- creating custom incoming 65
- Services, introduction 21
- SOCKS 71
  - and ICQ 72
  - and IRC 72
- SOCKS and AOL Messenger 72
- Static IP address 98, 99
- Static IP address, reason for 101

## T

- TCP/IP
  - releasing IP configuration 46
  - setting in Macintosh 29
  - setting in Unix, Linux, etc. 29
  - setting in Windows '95, '98 29
- Troubleshooting 99
  - checking link LED 105
  - connecting more than two offices 102
  - pinging 102
  - static IP address 101

## U

- Unix, setting TCP/IP 29
- URL database 85
- Using the manual 3

## V

- Virtual Private Networking
  - introduction 97

## W

- WebBlocker
  - categories 93
  - searching for blocked sites 96
  - The Learning Company 93
- Windows '95/'98/NT, disabling HTTP proxy 30

## Free Manuals Download Website

<http://myh66.com>

<http://usermanuals.us>

<http://www.somanuals.com>

<http://www.4manuals.cc>

<http://www.manual-lib.com>

<http://www.404manual.com>

<http://www.luxmanual.com>

<http://aubethermostatmanual.com>

Golf course search by state

<http://golfingnear.com>

Email search by domain

<http://emailbydomain.com>

Auto manuals search

<http://auto.somanuals.com>

TV manuals search

<http://tv.somanuals.com>