
WatchGuard SOHO WebBlocker

WatchGuard SOHO WebBlocker is an optional feature of the WatchGuard SOHO and SOHOtc that provides Web site filtering capabilities. It enables you to exert fine control over the types of Web sites users on your private network are allowed to view.

How WebBlocker Works

WebBlocker relies on a URL database built and maintained by The Learning Company for the 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.

WatchGuard copies the database to our Web site at regular intervals. Every time a user on your private network attempts to reach an Internet Web site, the SOHO queries our database and determines whether or not to block the site. Depending on conditions, the SOHO decides whether or not to block the site:

Web Site Not in CyberPatrol List

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

Web Site in CyberPatrol List

If the site is in our database at WatchGuard, 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.

Bypassing the SOHO WebBlocker

Ocasionally you may want to allow select individuals to bypass the filtering functions of the SOHO WebBlocker. For example, if you are using the SOHO in a home as a telecommuter, you may want to block a 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 private network who should be able to bypass the 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. Once 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 the SOHO WebBlocker

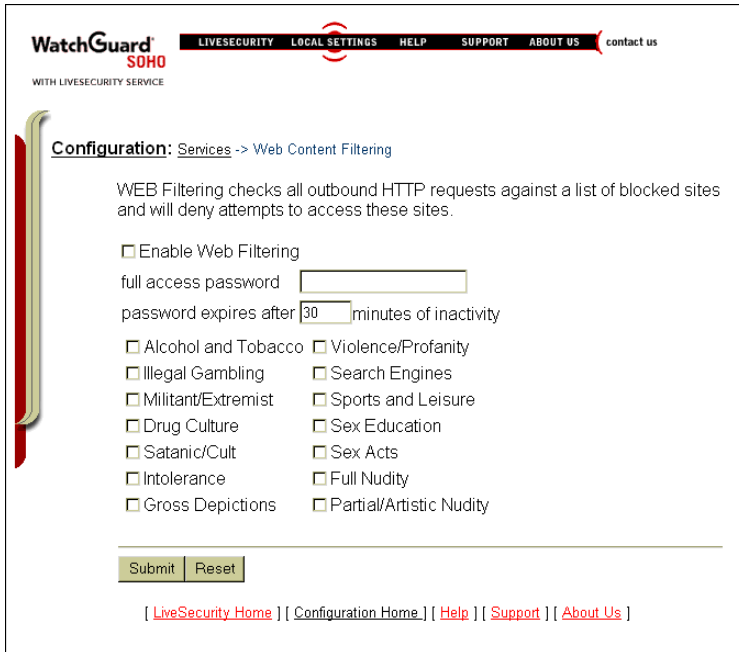
To use WatchGuard SOHO WebBlocker, you must first purchase and enable the WebBlocker feature key.

1. Open your Web browser to the WatchGuard SOHO LiveSecurity Service:
`http://bisd.watchguard.com/SOHO/Login.asp`
2. If you have already activated LiveSecurity, enter your User Name and Password and click Login. If you are a new user, follow instructions to activate your LiveSecurity Service.
3. Once logged in to LiveSecurity, click the WebBlocker link.
4. On the WebBlocker for SOHO Information page, click Buy Now.
5. Accept the end-user licence agreement, enter your credit card and billing information, then accept the order summary.
An order confirmation page appears and a new feature key is generated for your SOHO device. The next time the SOHO device reboots and contacts WatchGuard, it will obtain the new feature key and enable WebBlocker.
6. Reboot the SOHO.

Configuring the SOHO WebBlocker

Use the WatchGuard SOHO Configuration pages to enter settings for the SOHO WebBlocker. You must provide the location of the nearest WatchGuard WebBlocker server, a full access password for bypassing WebBlocker, the duration the full access password is valid, and the categories you wish to block.

1. Open a Web browser and enter the IP address to access the WatchGuard SOHO Configuration menu.
The default configuration IP address 192.168.111.1.
2. **Select Services.**
The Services menu appears.
3. **Select Web Blocking.**
The WebBlocker configuration page appears. It provides controls for activating and controlling WebBlocker, as well as checkboxes to determine which content types can be accessed.



WatchGuard
SOHO
WITH LIVESECURITY SERVICE

LIVESECURITY LOCAL SETTINGS HELP SUPPORT ABOUT US contact us

Configuration: Services -> Web Content Filtering

WEB Filtering checks all outbound HTTP requests against a list of blocked sites and will deny attempts to access these sites.

Enable Web Filtering

full access password

password expires after minutes of inactivity

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

[[LiveSecurity Home](#)] | [[Configuration Home](#)] | [[Help](#)] | [[Support](#)] | [[About Us](#)]

4. Check the **Enable Web Filtering** checkbox.
This turns on SOHO WebBlocker.
5. Enter the **Full Access Password**.
The Full Access Password provides users you select to enter a password that bypasses otherwise blocked sites.
6. Enter **Password Expiration duration in minutes**.
Setting the password expiration at, for example, 15 minutes, ensures that unattended Web browsers will be disconnected after sitting idle for 15 minutes. This ensures that only the individuals chosen to use the Full Access Password will be able to browse otherwise blocked sites.
7. Create your organization's **browsing profile**.
Enable the checkboxes for the categories to which you want to deny access.
8. Click the **Submit** button to register your changes.
Submitting the page alters your configuration file to turn on WebBlocker and block users from accessing Web sites that match the categories you checked in Step 8.

WebBlocker Categories

WebBlocker relies on a URL database built and maintained by The Learning Company for the CyberPatrol. The Learning Company constantly searches the Internet to update the list of blocked sites in each of 14 categories.



All of the categories pertain to advocacy rather than opinion and/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 which 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, on-line 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 criterion would not block sites describing typically illegal drugs that are legally prescribed for medicinal purposes (i.e., 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 soci-

ety 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 which 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 which 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 Google.

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. Excluded from this category are commercial sites selling sexual paraphernalia.

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 nudity or 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. Topic excludes all swimsuits, including thongs.

Communicating with CyberPatrol

At times, you may question whether or not a site is in the database WatchGuard receives from CyberPatrol. In addition, perhaps you find a site you would like to see added to the list. CyberPatrol maintains a Web site that enables you to directly query the database and provide feedback on its future growth.

Visiting the CyberPatrol Web Site

To learn more about the CyberPatrol CyberNOT Search Engine[®], you can visit their Web site at:

<http://www.cyberpatrol.com/cybernot>

At this site you can learn about how the database is maintained, more about the CyberLIST criteria, and how to appeal a blocked site or directory.

Verifying Whether a Web Site is in the WebBlocker Database

Use the CyberNOT Search Engine to search for specific Web sites and determine whether or not they are included in the database used by WatchGuard.

1. Open a Web browser to:

<http://www.cyberpatrol.com/cybernot/default.htm>

-
-
2. Scroll down to display the Cyber Patrol CyberNOT Search Engine.

Welcome to Cyber Patrol's CyberNOT Search Engine



Use our CyberNOT search engine, to check whether a URL is already on the CyberNOT list

Please enter the URL here:

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 request a site review.

Copyright and Patent Information

Copyright © 1996-2000 WatchGuard Technologies, Inc. All rights reserved.

WatchGuard SOHO, WatchGuard SOHOtc, and WebBlocker are either trademarks or registered trademarks of WatchGuard Technologies, Inc. in the United States and other countries. Firebox and LiveSecurity are trademarks of WatchGuard Technologies, Inc.

Other brands and their products are trademarks or registered trademarks of their respective holders and should be noted as such.

Cyber Patrol is a registered trademark of Learning Company Properties, Inc.

DocVer: B-2.1-WebBlocker-2