



Simply better network security.™

®

# **ThreatWall**

Web Proxy



## Copyright Notices

©eSoft, Inc. 2008. eSoft, InstaGate, and ThreatWall are registered trademarks, and SoftPak and SoftPak Director are trademarks of eSoft, Inc. Microsoft and Windows are registered trademarks of Microsoft Corporation. Netscape and Netscape Navigator are registered trademarks of Netscape Communications Corporation. Adobe, the Adobe logo, and Acrobat are registered trademarks of Adobe Systems Inc. UNIX is a registered trademark of UNIX Systems Laboratories, Inc. All other brand and/or product names are the property of their respective holders.

Portions of this software are covered under the GNU General Public License. You may freely obtain source code versions of the software covered by the GNU General Public License through the Internet at <http://www.redhat.com>. However, some applications remain the property of their owners, and require their permission to redistribute. For more information, access the eSoft web site at <http://www.esoft.com>.

Portions of this software are Copyright ” The Regents of the University of California. A complete copy of the copyright notice follows:

Copyright ” The Regents of the University of California.

All rights reserved.

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

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

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

All advertising materials mentioning features or use of this software must display the following acknowledgment:

“This product includes software developed by the University of California, Berkeley and its contributors.”

Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)

HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions of this software are Copyright ” The Apache Group. A complete copy of the copyright notice follows:

Copyright © 1995-1997 The Apache Group. All rights reserved.

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

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

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

All advertising materials mentioning features or use of this software must display the following acknowledgment:

“This product includes software developed by the Apache Group for use in the Apache HTTP server project (<http://www.apache.org/>).”

The names “Apache Server” and “Apache Group” must not be used to endorse or promote products derived from this software without prior written permission.

Redistributions of any form whatsoever must retain the following acknowledgment:

“This product includes software developed by the Apache Group for use in the Apache HTTP server project (<http://www.apache.org/>).”



# Web Proxy

## Proxy Settings

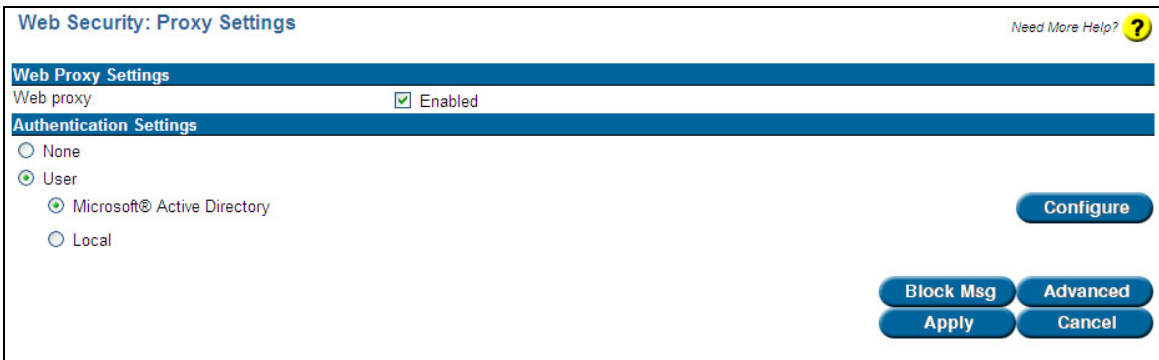
The web proxy allows you to control access to categorized sites. When enabled, each URL from a user's web browser is analyzed and based on the matching policy, either allowed or blocked. Even if you do not block access, enabling web proxy allows you to use the Web Security ThreatMonitor to view your users browsing habits.

There are two methods of authentication used to control user access:

- *None*. This option does not require user authentication but limits your ability to control different groups of users.
- *User*. If you enable this, you can control access by defining policies associated to different user groups.

### To configure web proxy:

1. From the *Web Security* menu, click *Web Proxy*.



2. Under *Web Proxy Settings*, check the *Web Proxy* checkbox to enable web proxy.
3. Under *Authentication Settings*, select the means of authorization to control user access:
  - *None*. No authentication from the client is required. Available options include:
    - *Transparent*. If the system is located on the network between your clients and router, check *Transparent* to intercept all web traffic without any browser configuration changes. If *Transparent* is unchecked, you will need to configure each client browser to connect to the system's IP address at port 8080.

- *User*. Each client must authenticate using a username and password. You must configure each client browser to connect to the system's IP address at port 8080. Available options include:
  - *Active Directory*. You must have configured *Remote Authentication* for Active Directory access. If you wish to use Active Directory but have not yet configured it, you can click *Configure* to go to Remote Authentication.
  - *Local*. Selecting *Local* uses only accounts defined on the system.
- 4. Click *Apply* to save your settings or click *Cancel* to exit without saving.

Once you have enabled web proxy, click *Advanced* to change non-standard configuration settings.

If you wish to customize the message that appears when a site is blocked, click *Block Msg*.

## Block Message

If access to a site is blocked, the user is redirected to the block message. This page shows them the full URL that was blocked and the associated categories.

If you wish, you can customize this page to better suit your organization.

To change the block message

1. From the *Web Security* menu, click *Web Proxy*.
2. From the Web Proxy form, click *Block Msg*.

**Web Security: Proxy Settings: Block Message** Need More Help? ?

**Custom Block Message**

When access to a site is denied, a web page with the following text will appear.

Title: ERROR: Access Denied by eSoft Web Security

Header 1: Access Denied by eSoft Web Security

Header 2:

Body: The following error was encountered:

Deny Message: Access Denied by eSoft Web Security

Contact: If you feel this is incorrect, please contact your administrator

Footer: Access control configuration prevents your request from being allowed at this time.

Apply Preview Cancel

3. Change the text in the desired field.
4. Click *Preview* to see the message as the user would see it. To close the preview, click *Close*.
5. Click *Apply* to save your settings or click *Cancel* to exit without saving.


## Proxy Settings, Advanced

The web proxy is properly configured to work in most environments. However, there are some cases where you may need or wish to change how it operates. The options you can change include:

- *Cache size.* This is the amount of disk space reserved by the proxy for managing static web content.
- *Access log.* This writes information about every connection made through the web proxy. Under normal circumstances it is disabled, but you may enable it if you use a 3rd party tool to analyze the data.
- *Allowed port settings.* Ports can be specified on a URL (such as *http://www.domain.com:80*). If they are not in the allowed port lists for either HTTP or HTTPS, they will not be allowed.
- *IP Address Filtering (only available if SiteFilter is installed).* Depending on your security concerns, you can control how the web proxy deals with URL where the domain is an IP address (such as *http://192.168.100.1*).
  - *Lookup in database.* The IP address will be looked up in the database for an associated category. If it is not found, it will be handled as Uncategorized.
  - *Block.* Deny any access to IP addresses.
  - *Allow.* Allow all access to IP addresses.
- *Parent Proxy.* You may specify an upstream web proxy server to pass all web traffic through. If required, you may also specify a username and password.
- *Enforce Google SafeSearch.* If enabled, forces all *google.com* and *google.co.uk* URLs will have Google's Safesearch parameters appended to them. This prevents users from viewing offensive sites and images through Google.
- *Default policies.* Under normal circumstances, the reserved policies (Block All and Full) are not shown from the Policies form. However if you wish to change these, you can access the Policies form with those reserved policies by clicking *Policies*. You can change the categories and names, but not the schedule nor delete the reserved policies


### To configure web proxy, advanced:

1. From the *Web Security* menu, click *Web Proxy*.
2. From *Web Proxy*, click *Advanced*.

**Web Security: Proxy Settings: Advanced** Need More Help? 

---




**Web Proxy Server Settings**




Cache size  

Access log  Enabled

---

**Allowed Port Settings**

Allowed ports    

Allowed SSL ports    

---

**IP Address Filtering Settings**

Lookup in database  
 Block  
 Allow

---



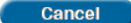
**Parent Proxy Settings**

Parent proxy  Enabled

---

**Safe Search**

Enforce Google Safe Search  Enabled

3. Change the appropriate fields.
4. Click *Apply* to save your settings or click *Cancel* to exit without saving.

## Custom Sites

Custom sites allow you to associate a list of URLs to a new or existing category. These can be used to either block access to matching URLs or allow access by overriding category associations defined by SiteFilter (if installed).

### Block

If you wish to block a site that is otherwise allowed, you can either create a new category (and associate it with a policy) or add to an existing category definition (requires SiteFilter).

For example, suppose you wish to block *www.badsite.com* and you already have a policy that blocks the category named *Bad Content*. Simply add the URL *www.badsite.com* to the *Bad Content* category.

Anyone associated with that policy will be blocked from accessing that URL.

### Allow

If you wish to allow access to a site that is otherwise blocked, you can create a new category but not block it with a policy.

For example, if you have SiteFilter installed, and a category you otherwise want to block also happens to block a URL you wish to allow, like *www.goodsite.com*, you can create a new category named *Good Content* and add *www.goodsite.com* to it. As long as you don't block the *Good Content* category in a policy, users will be able to access the site.

### Whitelist

You can also manage the special *Whitelist* category. This category is not allowed to be blocked by any policy and defines URLs that anyone can access at any time regardless of their web access settings.

For example, if you always wanted your users to access *www.alwaysallowed.com*, you can add this URL to the *Whitelist* category.


---

**NOTE: If you wish to block access to a custom site list, you must associate the category with a policy.**

---

### To configure custom sites:

1. From the *Web Security* menu, click *Custom Sites*.

**Web Security: Custom Sites** Need More Help? 

Category	Description	# of Sites
<input type="radio"/> Criminal Skills/Hacking (Criminal Activities)	Activities that violate human rights including murder, sabatoge, bomb building, etc. Information about illegal manipulation of electronic devices, encryption, misuse, and fraud. Warez and other illegal software distribution. Keywords: terrorism, torture, cracks, pirated software, copyright violation, evading law enforcement, lock-picking, burglary, gang Examples: warez.com, phreak.org	3
<input checked="" type="radio"/> Watch (Custom & Others)	Sites to watch from my organization.	1
<input type="radio"/> Whitelist	Accessible by any user regardless of web access permission.	3

2. If you wish to add a new custom site list, click *Add*.
3. If you wish to change an existing custom site list, select it and click *Modify*.
4. If you wish to delete an existing custom site list, select it and click *Delete*.

## Custom Sites Edit

To manage custom URL custom lists, you may add new lists or modify existing lists.

You may add an unlimited number of custom site lists and each list may contain an unlimited number of URLs.

### Sites

Each entry under Sites can contain a URL with a domain and/or path such as:

- *www.domain.com*
- *www.somesite.com/path*
- *www.anothersite.com/path/specificpage.html*

These can match any sub-domain or path. For example, *domain.com* will match *domain.com*, *www.domain.com*, *www.domain.com/path*, etc. However, *www.somesite.com/path* will not match *www.somesite.com*.

Alternatively, the entry can be a wildcard expression such as:

- *\*domain\**
- *somesite.com/\**

These wildcard expressions match any part of the URL. For example, *\*domain\** would match not only *domain.com*, *www.domain.com*, and *www.domain.com/path* but also *somedomain.com*, *www.anotherdomain.com/path*, etc.

### To add a new custom site list:

1. From the *Web Security* menu, click *Custom Sites*.
2. Click *Add*.

**Web Security: Custom Sites:Add** Need More Help? ?

**List Settings**

Category: Custom

Name: Watch

Description: Sites to watch from my organization

Sites: watch.com

Apply Cancel

3. If you wish to add to an existing category, select the desired category from the *Category* list.
4. If you wish to add a new category, from the *Category* list select *Custom*. New fields for Name and Description will appear.
5. Under *Sites*, specify all URLs you wish to associate with this category.
6. Click *Apply* to save your settings or click *Cancel* to exit without saving.

**To modify an existing custom site list:**

1. From the *Web Security* menu, click *Custom Sites*.
2. Select the radio button next to the category you wish to change and click *Modify*.

**Web Security: Custom Sites:Modify** Need More Help? ?

---

**List Settings**

Category	Whitelist
Sites	<pre>gooddomain.com goodpath.com/path goodpage.com/path/page.html</pre>

**Apply** **Cancel**

3. If this is a category you've created, you can change the *Name* and *Description*.
4. Under *Sites*, add or remove the desired URLs you wish to associate or disassociate from this category.
5. Click *Apply* to save your settings or click *Cancel* to exit without saving.

---

**NOTE: You may need to modify policies if you want to block these categories.**

---


## Custom Sites Delete

If you wish to remove a custom site list, delete it. All URLs associated with your custom site list will be removed.

If you delete a custom site list, it will be removed from any associated policy.

### To delete a custom site list:

1. From the *Web Security* menu, click *Custom Sites*.
2. Select the radio button next to the category you wish to delete.
3. Click *Delete*.

**Web Security: Custom Sites:Delete** Need More Help? 

Custom Sites Information	
Category	Criminal Skills/Hacking
Description	Activities that violate human rights including murder, sabatoge, bomb building, etc. Information about illegal manipulation of electronic devices, encryption, misuse, and fraud. Warez and other illegal software distribution. Keywords: terrorism, torture, cracks, pirated software, copyright violation, evading law enforcement, lock-picking, burglary, gang Examples: warez.com, phreak.org
Sites	baddomain.com badpath.com/path badpage.com/path/page.html

*Do you really want to delete this custom site list?*

4. A popup will appear.
5. Click *Yes* to delete the custom site list or click *No* to exit without deleting.

## Policies

A policy consists of:

- *Schedule*. The times for which the policy is active.
- *Blocked Categories*. All categories that the user will not be able to access during the scheduled time.

Policies are applied differently depending on the web proxy authentication setting:

- None. All policies are considered to be associated with all users.
- User. Policies must be associated with users through Group management.

One or more associated policies are combined to create the web security permission for each user. They are always combined to provide the *most restrictive access*.

### To configure policies:

1. From the *Web Security* menu, click *Policies*.

**Web Security: Policies** Need More Help? 

*All policies are combined to provide the global web security permission.*

Policy	Schedule	Blocked Categories
<input type="radio"/> <b>Afternoon and Evening</b>	Mon, Tue, Wed, Thu, Fri 1 PM — 12 AM	<ul style="list-style-type: none"> <li>Adult Materials (Subcategories: All)</li> <li>Communication (Subcategories: All)</li> <li>Criminal Activities (Subcategories: All)</li> <li>Entertainment (Subcategories: All)</li> <li>Games (Subcategories: All)</li> <li>Health (Subcategories: All)</li> <li>Miscellaneous (Subcategories: All)</li> <li>Shopping (Subcategories: All)</li> <li>Society (Subcategories: All)</li> <li>Spyware/ Adware (Subcategories: All)</li> <li>Custom &amp; Others (Subcategories: Uncategorized)</li> </ul>
<input checked="" type="radio"/> <b>Lunch</b>	Mon, Tue, Wed, Thu, Fri 11 AM — 1 PM	<ul style="list-style-type: none"> <li>Adult Materials (Subcategories: All)</li> <li>Criminal Activities (Subcategories: All)</li> <li>Spyware/ Adware (Subcategories: All)</li> <li>Custom &amp; Others (Subcategories: Uncategorized)</li> </ul>
<input type="radio"/> <b>Morning</b>	Mon, Tue, Wed, Thu, Fri 12 AM — 11 AM	<ul style="list-style-type: none"> <li>Adult Materials (Subcategories: All)</li> <li>Communication (Subcategories: All)</li> <li>Criminal Activities (Subcategories: All)</li> <li>Entertainment (Subcategories: All)</li> <li>Games (Subcategories: All)</li> <li>Health (Subcategories: All)</li> <li>Miscellaneous (Subcategories: All)</li> <li>Shopping (Subcategories: All)</li> <li>Society (Subcategories: All)</li> <li>Spyware/ Adware (Subcategories: All)</li> <li>Custom &amp; Others (Subcategories: Uncategorized)</li> </ul>
<input type="radio"/> <b>Weekend</b>	Sun, Sat 12 AM — 12 AM	<ul style="list-style-type: none"> <li>Adult Materials (Subcategories: All)</li> <li>Criminal Activities (Subcategories: All)</li> <li>Spyware/ Adware (Subcategories: All)</li> <li>Custom &amp; Others (Subcategories: Uncategorized)</li> </ul>

Add Modify Delete Copy Done

2. If you wish to add a new policy, click *Add*.
3. If you wish to change an existing policy, select it and click *Modify*.
4. If you wish to delete an existing policy, select it and click *Delete*.

## Policies Edit

For each policy, you can control the following:

- *Name*. This identifier will be used in other parts of the system such as group management and the Web Security ThreatMonitor.
- *Schedule*. This can either be *All days, all hours*, or you can select *Custom* to choose begin and end time for each day of the week.
- *Blocked Categories*. If you choose *All Defined*, this means that all categories, including any new ones you might add in the future, will be blocked. Under normal circumstances you will want to use *Select* to pick specific categories to block.

### Selected Blocked Categories

This table shows all available categories that are defined through custom sites or those included with the SiteFilter database (if SiteFilter is installed). You can select individual categories or entire category groups. If you move your mouse over a category, you will see a tooltip description of the category.

### To add a new policy

1. From the *Web Security* menu, click *Policies*.
2. Click *Add*.

[Need More Help?](#)

### Web Security: Policies: Add

**Policy Settings**

Name

**Schedule**

All days, all hours  
 Custom

**Custom Schedule**

Day	Start At	Finish At
Sunday	None	—
Monday	11 AM	1 PM
Tuesday	11 AM	1 PM
Wednesday	11 AM	1 PM
Thursday	11 AM	1 PM
Friday	11 AM	1 PM
Saturday	None	—

**Blocked Categories**

All defined  
 Selected

**Selected Blocked Categories**

<input checked="" type="checkbox"/> <b>Adult Materials</b>	<input checked="" type="checkbox"/> Hate Speech	<input type="checkbox"/> Anonymizer	<input type="checkbox"/> Shopping
<input checked="" type="checkbox"/> Mature	<input checked="" type="checkbox"/> Illegal Drugs	<input type="checkbox"/> Computers and Technology	<input type="checkbox"/> <b>Society</b>
<input checked="" type="checkbox"/> Nudity	<input type="checkbox"/> <b>Education</b>	<input type="checkbox"/> Download Sites	<input type="checkbox"/> Cars/Transportation
<input checked="" type="checkbox"/> Pornography/Sex	<input type="checkbox"/> Education	<input type="checkbox"/> Translator	<input type="checkbox"/> Dating
<input checked="" type="checkbox"/> Violence	<input type="checkbox"/> <b>Entertainment</b>	<input type="checkbox"/> <b>Miscellaneous</b>	<input type="checkbox"/> Home/Leisure
<input checked="" type="checkbox"/> Weapons	<input type="checkbox"/> Art	<input type="checkbox"/> Miscellaneous	<input type="checkbox"/> Personal Webpages
<input type="checkbox"/> <b>Business/ Services</b>	<input type="checkbox"/> Entertainment and Videos	<input type="checkbox"/> <b>News</b>	<input type="checkbox"/> Restaurants
<input type="checkbox"/> Business/Services	<input type="checkbox"/> Humor	<input type="checkbox"/> News	<input type="checkbox"/> Sports and Recreation
<input type="checkbox"/> Finance	<input type="checkbox"/> Music	<input type="checkbox"/> <b>Politics/ Religion/ Law</b>	<input type="checkbox"/> Travel
<input type="checkbox"/> Job Search	<input type="checkbox"/> <b>Games</b>	<input type="checkbox"/> Government	<input checked="" type="checkbox"/> <b>Spyware/ Adware</b>
<input type="checkbox"/> Real Estate	<input type="checkbox"/> Gambling	<input type="checkbox"/> Military	<input checked="" type="checkbox"/> Adware
<input type="checkbox"/> <b>Communication</b>	<input type="checkbox"/> Games	<input type="checkbox"/> Non-profits	<input checked="" type="checkbox"/> Compromised
<input type="checkbox"/> Chat/IM	<input type="checkbox"/> <b>Health</b>	<input type="checkbox"/> Politics and Law	<input checked="" type="checkbox"/> Phishing/Fraud
<input type="checkbox"/> Community Sites	<input type="checkbox"/> Alcohol	<input type="checkbox"/> Religion	<input checked="" type="checkbox"/> Spam
<input type="checkbox"/> Social Networking	<input type="checkbox"/> Health	<input type="checkbox"/> <b>Search Engines</b>	<input checked="" type="checkbox"/> Spyware and Malicious Sites
<input type="checkbox"/> Web-based Email	<input type="checkbox"/> Pharmacy	<input type="checkbox"/> Portal Sites	<b>Custom &amp; Others</b>
<input checked="" type="checkbox"/> <b>Criminal Activities</b>	<input type="checkbox"/> Tobacco	<input type="checkbox"/> Search Engines	<input checked="" type="checkbox"/> Uncategorized
<input checked="" type="checkbox"/> Criminal Skills/Hacking	<input type="checkbox"/> <b>Information Technology</b>	<input type="checkbox"/> Shopping	<input type="checkbox"/> Watch

3. Specify the *Name* of the policy.
4. Specify the desired *Schedule* settings.
5. Specify the desired *Category* settings.
6. Click *Apply* to save your settings or click *Cancel* to exit without saving.

#### To modify an existing policy:

1. From the *Web Security* menu, click *Policies*.
2. Select the radio button next to the policy you wish to change and click *Modify*.

**Web Security: Policies: Modify** Need More Help?

---

**Policy Settings**

Name

---

**Schedule**

All days, all hours  
 Custom

---

**Custom Schedule**

Day	Start At	Finish At
Sunday	None	—
Monday	Midnight	11 AM
Tuesday	Midnight	11 AM
Wednesday	Midnight	11 AM
Thursday	Midnight	11 AM
Friday	Midnight	11 AM
Saturday	None	—

---

**Blocked Categories**

All defined  
 Selected

---

**Selected Blocked Categories**

<input checked="" type="checkbox"/> <b>Adult Materials</b> <input checked="" type="checkbox"/> Mature <input checked="" type="checkbox"/> Nudity <input checked="" type="checkbox"/> Pornography/Sex <input checked="" type="checkbox"/> Violence <input checked="" type="checkbox"/> Weapons <input type="checkbox"/> <b>Business/ Services</b> <input type="checkbox"/> Business/Services <input type="checkbox"/> Finance <input type="checkbox"/> Job Search <input type="checkbox"/> Real Estate <input checked="" type="checkbox"/> <b>Communication</b> <input checked="" type="checkbox"/> Chat/IM <input checked="" type="checkbox"/> Community Sites <input checked="" type="checkbox"/> Social Networking <input checked="" type="checkbox"/> Web-based Email <input checked="" type="checkbox"/> <b>Criminal Activities</b> <input checked="" type="checkbox"/> Criminal Skills/Hacking	<input checked="" type="checkbox"/> Hate Speech <input checked="" type="checkbox"/> Illegal Drugs <input type="checkbox"/> <b>Education</b> <input type="checkbox"/> Education <input checked="" type="checkbox"/> <b>Entertainment</b> <input checked="" type="checkbox"/> Art <input checked="" type="checkbox"/> Entertainment and Videos <input checked="" type="checkbox"/> Humor <input checked="" type="checkbox"/> Music <input checked="" type="checkbox"/> <b>Games</b> <input checked="" type="checkbox"/> Gambling <input checked="" type="checkbox"/> Games <input checked="" type="checkbox"/> <b>Health</b> <input checked="" type="checkbox"/> Alcohol <input checked="" type="checkbox"/> Health <input checked="" type="checkbox"/> Pharmacy <input checked="" type="checkbox"/> Tobacco <input type="checkbox"/> <b>Information Technology</b>	<input type="checkbox"/> Anonymizer <input type="checkbox"/> Computers and Technology <input type="checkbox"/> Download Sites <input type="checkbox"/> Translator <input checked="" type="checkbox"/> <b>Miscellaneous</b> <input checked="" type="checkbox"/> Miscellaneous <input type="checkbox"/> <b>News</b> <input type="checkbox"/> News <input type="checkbox"/> <b>Politics/ Religion/ Law</b> <input type="checkbox"/> Government <input type="checkbox"/> Military <input type="checkbox"/> Non-profits <input type="checkbox"/> Politics and Law <input type="checkbox"/> Religion <input type="checkbox"/> <b>Search Engines</b> <input type="checkbox"/> Portal Sites <input type="checkbox"/> Search Engines <input checked="" type="checkbox"/> <b>Shopping</b>	<input checked="" type="checkbox"/> Shopping <input checked="" type="checkbox"/> <b>Society</b> <input checked="" type="checkbox"/> Cars/Transportation <input checked="" type="checkbox"/> Dating <input checked="" type="checkbox"/> Home/Leisure <input checked="" type="checkbox"/> Personal Webpages <input checked="" type="checkbox"/> Restaurants <input checked="" type="checkbox"/> Sports and Recreation <input checked="" type="checkbox"/> Travel <input checked="" type="checkbox"/> <b>Spyware/ Adware</b> <input checked="" type="checkbox"/> Adware <input checked="" type="checkbox"/> Compromised <input checked="" type="checkbox"/> Phishing/Fraud <input checked="" type="checkbox"/> Spam <input checked="" type="checkbox"/> Spyware and Malicious Sites <b>Custom &amp; Others</b> <input checked="" type="checkbox"/> Uncategorized <input type="checkbox"/> Watch
--	--	--	---

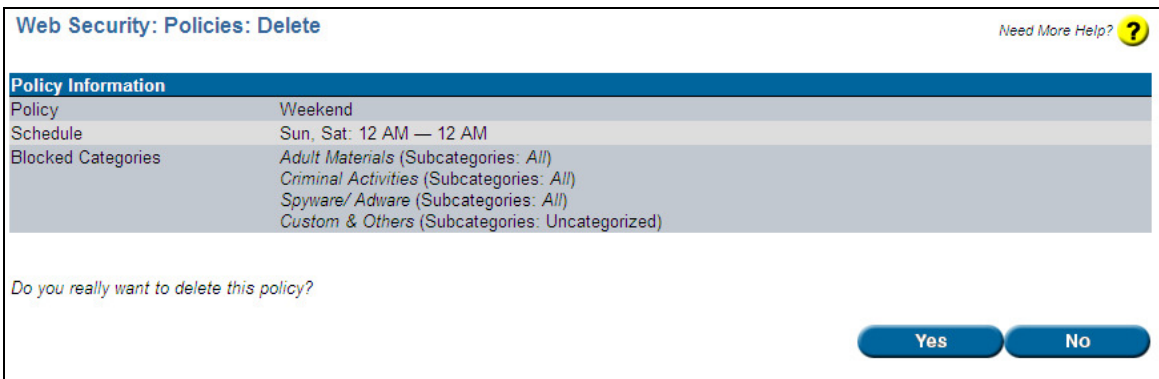
3. If you wish, change the *Name* of the policy.
4. If you wish, change the *Schedule* settings.
5. If you wish, change the *Category* settings.
6. Click *Apply* to save your settings or click *Cancel* to exit without saving.

## Policies Delete

After you've deleted the policy, it will be removed from any associated user groups.

### To delete a policy:

1. From the *Web Security* menu, click *Policies*.
2. Select the radio button next to the policy you wish to delete.
3. Click *Delete*.



4. A popup will appear asking for confirmation.
5. Click *Yes* to delete the policy or click *No* to exit without deleting.

## Updates

New additions to the SiteFilter database are checked periodically and automatically downloaded. You can change the interval or force an immediate check.

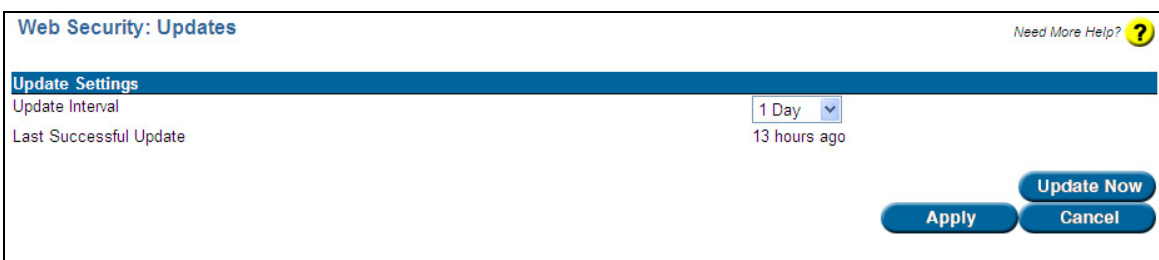
---

**NOTE: You will only see this option if you are subscribed to SiteFilter.**

---

### To change the interval:

1. From the *Web Security* menu, click *Updates*.



2. Next to *Update Interval*, select a new interval to perform checks.
3. Click *Apply* to save your settings or click *Cancel* to exit without saving.

### To check immediately:

1. From the *Web Security* menu, click *Updates*.
2. Click *Update Now*


You will see a progress bar that indicates the progress of downloading and installing the new database or database updates.

## Category

Occasionally you may come across a URL that is not categorized correctly. You can correct this.

### To recategorize a site:

1. Go to the *Web Security ThreatMonitor*.
2. From either the *Recent Activity* or *Recent Activity, Detailed* reports, click *Category* next to the URL you wish to change.

**Web Security Monitor: Categorize** Need More Help? 

---

**Site Categorization**

Site Address

---

**Categories**

<p><b>Adult Materials</b></p> <input type="checkbox"/> Mature <input type="checkbox"/> Nudity <input type="checkbox"/> Pornography/Sex <input type="checkbox"/> Violence <input type="checkbox"/> Weapons	<p><input type="checkbox"/> Hate Speech  <input type="checkbox"/> Illegal Drugs</p> <p><b>Education</b></p> <input checked="" type="checkbox"/> Education	<p><input type="checkbox"/> Anonymizer  <input type="checkbox"/> Computers and Technology  <input type="checkbox"/> Download Sites  <input type="checkbox"/> Translator</p> <p><b>Miscellaneous</b></p> <input type="checkbox"/> Miscellaneous	<p><input type="checkbox"/> Shopping</p> <p><b>Society</b></p> <input type="checkbox"/> Cars/Transportation <input type="checkbox"/> Dating <input type="checkbox"/> Home/Leisure <input type="checkbox"/> Personal Webpages <input type="checkbox"/> Restaurants <input type="checkbox"/> Sports and Recreation <input type="checkbox"/> Travel
<p><b>Business/ Services</b></p> <input type="checkbox"/> Business/Services <input type="checkbox"/> Finance <input type="checkbox"/> Job Search <input type="checkbox"/> Real Estate	<p><b>Entertainment</b></p> <input type="checkbox"/> Art <input type="checkbox"/> Entertainment and Videos <input type="checkbox"/> Humor <input type="checkbox"/> Music	<p><b>News</b></p> <input type="checkbox"/> News	<p><b>Politics/ Religion/ Law</b></p> <input type="checkbox"/> Government <input type="checkbox"/> Military <input type="checkbox"/> Non-profits <input type="checkbox"/> Politics and Law <input type="checkbox"/> Religion
<p><b>Communication</b></p> <input type="checkbox"/> Chat/IM <input type="checkbox"/> Community Sites <input type="checkbox"/> Social Networking <input type="checkbox"/> Web-based Email	<p><b>Games</b></p> <input type="checkbox"/> Gambling <input type="checkbox"/> Games	<p><b>Politics/ Religion/ Law</b></p> <input type="checkbox"/> Government <input type="checkbox"/> Military <input type="checkbox"/> Non-profits <input type="checkbox"/> Politics and Law <input type="checkbox"/> Religion	<p><b>Spyware/ Adware</b></p> <input type="checkbox"/> Adware <input type="checkbox"/> Compromised <input type="checkbox"/> Phishing/Fraud <input type="checkbox"/> Spam <input type="checkbox"/> Spyware and Malicious Sites
<p><b>Criminal Activities</b></p> <input type="checkbox"/> Criminal Skills/Hacking	<p><b>Health</b></p> <input type="checkbox"/> Alcohol <input type="checkbox"/> Health <input type="checkbox"/> Pharmacy <input type="checkbox"/> Tobacco	<p><b>Search Engines</b></p> <input type="checkbox"/> Portal Sites <input type="checkbox"/> Search Engines	<p><b>Custom &amp; Others</b></p> <input type="checkbox"/> Uncategorized
	<p><b>Information Technology</b></p>	<p><b>Shopping</b></p>	

3. Uncheck the categories that should not be associated with the URL.
4. Check the categories that should be associated with the URL.
5. Click *Apply* to save the change. Click *Cancel* to exit without saving the change.