

M86 Web Filter EVALUATION GUIDE Models: 300, 500, 700

Software Version: 4.0.10 Document Version: 06.22.10

M86 WEB FILTER EVALUATION GUIDE FOR 300, 500, 700 MODELS

© 2010 M86 Security

All rights reserved. Printed in the United States of America

Local: 714.282.6111 • Domestic U.S.: 1.888.786.7999 • International: +1.714.282.6111

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine readable form without prior written consent from M86 Security.

Every effort has been made to ensure the accuracy of this document. However, M86 Security makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. M86 Security shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. Due to future enhancements and modifications of this product, the information described in this documentation is subject to change without notice.

Trademarks

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Part# WF-EG-100622

CONTENTS

WEB FILTER EVALUATION GUIDE	1
Market Overview	1
Product Overview	1
Note to Evaluators.	2
INSTALL THE WEB FILTER, UPDATE LIBRARIES	3
CONFIGURE AND TEST THE WEB FILTER	4
Understand the most common and useful features.	4
Group setup for different user types on the network	5
Apply different filtering levels for different types of users	
How to create an IP Group	6
How to define members for this IP Group	6
Rules and Profiles: Creating and using each	
How is a Rule used?	7
How is a Profile used?	8
How to create a new Rule .	
Global Group Profile	11
Set the Global Group Profile	
Create, edit a list of selected Categories	
Group Profile	
Set the Group Profile	
Create, edit a list of selected Categories for a Group Profile	13
Group settings tests	14
Test the Rules and Profiles feature	
Test the Rule	
Custom Categories	
Create and configure a Custom Category	
How to create a Custom Category	
How to add URLs to the Custom Category	
Custom Category setup and usage test	
Filtering profile features	18
Time Profile feature	
Set up a Time Profile	
Test the Time Profile	
Quota feature	
Set up the Quota feature	
Test the Quota feature	
White List feature	
How to create and configure a White List	
Test the White List	
Warn feature	
How to test the Warn feature	
Google/Bing/Yahoo!/Youtube/Ask/AOL Safe Search Enforcement	
How to configure the Safe Search Enforcement feature	

How to test the Safe Search Enforcement feature	24
Search Engine Keyword Filtering	25
How to configure Search Engine Keyword Filtering	25
How to test Search Engine Keyword Filtering	26
Attachment filtering	27
How to configure attachment filtering	27
How to test attachment filtering	
Wildcard filtering	
How to configure wildcard filtering	29
How to test wildcard filtering	30
Configure, test, block services	31
Anonymous proxies	
How to configure anonymous proxies	
How to test anonymous proxies	
Block IM, P2P applications and streaming media	
Configure IM, P2P, streaming media blocking	
How to test for IM	
How to test for P2P	
How to test for streaming media	34
Real Time Probes and X-Strikes Blocking	
Real Time Probes feature	
How to configure Real Time Probes	
How to test Real Time Probes	
X-Strikes feature	
How to configure the X-Strikes feature	
How to test X-Strikes	40

WEB FILTER EVALUATION GUIDE

Market Overview

In order to survive in today's world, businesses continually come up with new products, more sales, and better service. But most often, the corporate world is financially threatened from the inside. Employees harm businesses when they view pornography and other offensive Web content at work, which often result in sexual and hostile work environment lawsuits. Organizations also lose time and money when employees tie up network bandwidth with IM and P2P, and/or allow spyware and malware into the system. And finally, a host of federal and state laws require that organizations protect customer data, or risk severe penalties.

Filtering comes down to four simple objectives: Mitigate legal liabilities created by inappropriate Web content; increase productivity by removing Internet distractions; protect the network from threats delivered by Internet services and applications; and preserve network resources. M86 Security has more than 10 years of pioneering leadership in filtering technology and is widely recognized as the premier appliance-based filtering solution on the market. The M86 Web Filter solution features single-source support, simple and straight-forward pricing, and product design that meets the needs of a wide range of filtering expectations.

M86 Security offers a wide range of Internet filtering and reporting appliances that not only help companies maintain compliance with laws such as the California Security Breach Information Act (CSBIA) (see http://www.8e6.com/resources/ internet-security-compliance-laws/), but also help protect the security of a company's network infrastructure. With no premiums, easy to install and use, and 24-7 technical support, M86 Security is the perfect choice for overburdened IT administrators and managers.

Product Overview

Thank you for choosing to review the M86 Web Filter. The Web Filter tracks end users' online activity and can be configured to block specific Web sites or service ports, thereby protecting organizations against lost productivity, constricted bandwidth and possible legal liability resulting from Internet content.

This product also features expansive content categories (called libraries), instant message and peer-to-peer blocking, user authentication, and intuitive administrative navigation. All of these features are provided in a true appliance that provides speed and stability unmatched by any software product. In addition, the Web Filter is fail-safe giving administrators the peace of mind that filtering won't ever impact the network's performance—or shut it down.

The Web Filter appliance is designed to complement existing security measures by providing protection from threats *inside* the network—the threats most often unseen and discovered too late.

Note to Evaluators

Thank you for taking the time to review M86's Web Filter appliance. Your interest in our company and product is greatly appreciated.

This Evaluation Guide Is designed to provide product evaluators an efficient way to install, configure and exercise the main product features of the Web Filter.

INSTALL THE WEB FILTER, UPDATE LIBRARIES

To install the appliance, configure the application, and test filtering, please refer to the step-by-step instructions found in the **M86 Web Filter Installation Guide** provided in the shipping carton.

We also recommend, prior to reviewing the Web Filter that you perform a complete library update.

This is done by going into the Web Filter Administrator console.

- 1. Click the Library link at the top of the screen.
- 2. From the navigation panel, click Updates and select Manual Update from the pop-up menu.
- 3. In the Manual Update to M86 Supplied Categories window, click the radio button corresponding to **Complete Update**.
- 4. Click **Update Now** to begin the update process.

CONFIGURE AND TEST THE WEB FILTER

Understand the most common and useful features

One of the advantages of a hardware appliance, in addition to its compatibility and extremely low profile on the network, is its ease of use. Configuration of the Web Filter can seem disarmingly simple at times, but when the hardware and software are designed to work together, the levels of complication decrease and robust power and efficiency significantly increase.

One of the challenges of simplicity is that it offers little variation in the appearance of the interface used to administer the Web Filter. Spending only a short time configuring and customizing the many capabilities of the Web Filter quickly overcomes any confusion related to this simple similarity, and the following exercises are meant to provide a very explicit and easy-to-follow way to become comfortable with the administrator console.

This section of the evaluation manual is to guide the evaluator, in a linear fashion, through the most common and useful features of the Web Filter, starting with the elements that should be configured first and continuing with features that require an understanding of the steps learned while configuring those first elements. Once one gets the basic flow of how filtering options are set up, it becomes quite simple to quickly make adjustments, if needed. And, the Web Filter's incredible capacity to be configured once and left alone, or to support extensive customization and specialization, make it the most versatile and network friendly filter on the market.

Group setup for different user types on the network

Apply different filtering levels for different types of users

Description: There are two primary Groups to understand when administering the Web Filter. The first, the **Global Group**, sets the default filtering policy for all users. In other words, the Global Group's set of filtering parameters (called a profile, to be explained later) governs every user's Internet access restrictions and permissions, *unless* a user or a group that user belongs to, has been assigned custom filtering parameters. Those exceptions to the Global Group (and there can be many) are simply called **Groups**. For example, setting aside an IP range for the sales department and altering their filtering restrictions and permissions would be considered creating a Group, likely called something as generic as Sales, and represented as an IP subset in the Global Group tree.

Policy L	rary Reporting System Help Logout Web Filter	186
	(Fg.) @ 2010/02	V00 15:50:40
Group	Bisplay Help Topics for the Policy section	
T .C	The Policy section is comprised of windows and dislog boxes used for adding and maintaining master IP groups or LDAP domains, and for streating filtering profiles for groups, u containers, and/or vortications.	(ers,
	For the IP proup option, the global administrator relates master IP groups. Within each individual IP group, the designated IP Group administrator adds sub-groups and individual members, and relates and maintains their fittering profiles.	UP
	For LDAP domains, the global administrator must finat set up authentication in the Oystem section in voter to enable LDAP options. The global administrator then adds an LDAP of this section, and possibly adds one or more entities to the LDAP branch of the global administrator to adding a	
	The navigation panel at the left of the screen contains a hierarchical list of groups set up in a tree format. At the root of this tree is Policy. The main branches of the tree include: Oil and IP group, followed by LDAP if authentication is enabled. IPLDAP group administrators will only see the branch(es) of the tree containing entities a signed to himber. NOTE: Is synchronization feature is used and the Wrob Filter is set up in the Target mode to synchronize both profile and sizeray setting changes, group administrators will not see any branc tree. With this section applied, global administrators will only see the Olecal Orceo Range to Detection;	f the
	Double-click the branch of your selection to display the list of groupsidomains previously added to that branch. Keep double-clicking items in the tree list to view additional items.	
	Click an entity in the tree list to view a menu of topics or actions that can be performed for the selected entity.	
	For help in any window, mouse-over the "?" symbol to view information about that window, or press F1. Press F5 to refresh the console.	
	For additional information about this current section of the console, click the link above this window to view Help Topics.	
	To navigate to another section of the console, click the tab at the top of the screen for Home, Library, Reporting, System, or Help, Click Logout to exit the console.	
-20-77		

The main Policy screen

The **POLICY** administrative feature on the Web Filter allows the administrator maximum control over setting appropriate filtering levels across a broad spectrum of users. In the work environment, this could be represented by sales, accounting, research, marketing and shipping all sharing the same IP range, but requiring different levels of filtering. The POLICY feature allows the administrator to set up these groups, assign custom filtering parameters to each, and adjust those parameters as needed.

Configuration: For the purpose of evaluating the ease and effectiveness of the Web Filter's group filtering, the following example addresses the most common configuration—grouping by IP address. The Web Filter can also group by LDAP domains. Should you wish to test the group features in one of these configurations, please refer to the M86 Web Filter Authentication User Guide, available from the M86 Security Web site. The setup is not complicated, but there are system settings required that must be initiated prior to establishing the groups in these environments, and it will be helpful and save time to work with a Solutions Engineer the first time these settings are initiated.

How to create an IP Group

- 1. Navigate the top level administrator console to POLICY.
- 2. Click on IP and select Add Group.
- 3. Provide the appropriate Group name (use AllUsers for this evaluation) and supply a password for this group. Click **OK**.

How to define members for this IP Group

100		BECURIT
IP : AllUsers : Me	mbers M	張 是 2010/06/25 09(2
lobal Group	Add members by @ P @ SubGroup	
AlUsers	IP/MAL. Members When using Taddesses to identify groups on the network, the IP address and network or IP range for the designated member must in this frame by entering the IP address and retemak or IP start and P end, and then claim Add. Use the claidate to calculate P address, and then claim Add. Once a member addres, a sub-group can be created and defined.	t first be entered in the Range to Detect global group window. A member IP is ad ranges without overlaps. A member MAC is added in this frame by entering the M
	Current Members	
	192.100.20.024	
		Remove
	New Members G Source P C Source P Start C Source P Start C Source P Start C Source PAC	

IP group members

- 1. Click the newly created Group and select Members.
- 2. Add members to this Group by either an IP Range or Subnet within the Range to Detect parameters of the Global Group defined earlier when setting up the Web Filter. These IP Addresses should be the IP Addresses of the computers filtered for the purposes of your testing.

Rules and Profiles: Creating and using each

Description: Rules and Profiles may seem confusing as it often appears that they are used interchangeably. And, while the administrative windows controlling the creation of Rules and Profiles are very similar, they each serve two distinct purposes.

NOTE: The general rule of thumb: A Rule can be applied to a Profile, but a Profile can't be applied to a Rule. A Rule is a custom configuration of Blocked, Passed, Warned, and Always Allowed categories. A Profile contains the particular filtering parameters that are unique to a group or individual, and consists of Library Categories, Rules, Ports and numerous other filtering features that can be turned on or off.

How is a Rule used?

A Rule is a custom set of Library Categories. For example RuleX can be named LegalLiability and be set to block the library categories Pornography/Adult Content, Child Pornography, Explicit Art, Obscene and Tasteless, and R-Rated.

This Rule is then saved, eliminating the need to rebuild that set of Library Categories the next time that same particular set of categories needs to be applied to a group or individual. The Rule becomes part of a Profile that defines the filtering parameters for a group or individual.

Allineen	tegory Profile 😡				105	2 2010/06/25
al Group ogo NUCers P	Cologory Patients to Cologory Radients URL Filter Options Groups Allibles : Ourset Profile Minimum Filtering Level Available Filter Levels Rulco Minimum Filtering Level *				M	inimum Filteri hid Pornography ornography/Adut O
	Rule Details				1	
	Category	Pass	Allow	Warn	Block	Quota
	Category Groups		<u> </u>			
	E 🔂 Adult Content					
	Bandwidth	<u>Q</u>				
	🗉 🙆 Business/Investments	<u></u>			and the second s	
	E Community/Organizations	<u> </u>			-	
	Education	<u> </u>				
	Contentairment	<u></u>			-	
	Government/Law/Politics	<u></u>			-	
	E C Heath-Fitness				and the second second	
	🕀 🎃 llegal/Guestionable	<u> </u>				
	Contration Technology	<u> </u>	1		-	
	Itemet Communication	<u></u>			-	
	Internet Productivity	8		-	-	
	Internet/Intranet Misc.	<u>×</u>			-	
	NewsReports	<u>v</u>			-	
	Religion/Beliefs	×			-	
	B Ca Securty	X	-		-	
	B Shopping	<u>8</u>	-		-	
	R Cociety & Hentyles	8				
	TravelEvents	<u>×</u>		_	-	
	🕀 🚞 Custom Categories			-		
	Uncategorized Sites Pass 💌				Overall (Q 👻 IIO etouc
						0

Rule tab in profile window

How is a Profile used?

A Profile defines the particular filtering parameters assigned to a group or individual. There are two kinds of Profiles. The first is the **Global Group Profile**.

Alliners : Cate	any Profile Q					\$ @ 2010/06/25 C
ibal Group Iogo AllUsers AP	Category Restrect LRL, Filter Options] Group: Allisters Current Profile Minimum Filtering Level Available Filter Levels Custon Profile					Minimum Filtering Child Pornography Pornography/Adult Con
	Rule Details Category	Dava	Alleyer	Warn	Block	Quata
	Cological Cological Cologi	000000000000000000000000000000000000000			0.4	al Conto (III Y) (P

Category Profile tab

The default for the Global Group Profile is set up under the Category Profile tab of the Global Group's administrative controls. Its default is set at custom and uncategorized sites are not blocked (note the Uncategorized Sites pull-down menu at the bottom of the window). The custom setting allows the administrator to immediately assign Library Categories to be passed, always allowed, warned or blocked to establish the initial default level of filtering assigned to every user (IP address) until that user (IP address) is assigned a sub-group or individual profile. *The Global Group Profile setting doesn't use Rules, only library categories.*

The second profile is the **Group Profile**. A Group Profile is assigned to an IP Group under the Global Group and can contain filtering parameters different from the Global Group default. For example, a company may have a Global Group Profile that blocks access to all sites in the earlier LegalLiability Rule example, i.e. Pornography/Adult Content, Child Pornography, Explicit Art, Obscene and Tasteless, and R-Rated. That means every employee (or every computer the employees use) is subject to those filter parameters. However...

Let's say the employees in the marketing department need to access photo services, online publications and other sites that might contain some adult content —or at least suggestive images. An administrator can set up a Group that is subject to a custom profile, which might be called Marketing, which is different* from the Global Group Profile, to allow access to the R-Rated library category. This group, or range of IP addresses, now exists within the Global Group, but with different filtering criteria. The rest of the Global Group (all other IP addresses) remain filtered by the default Global Group Profile, which includes R-Rated. **NOTE**: * Different doesn't necessarily mean that a group is no longer filtered by the library Categories in the Global Group Profile. In fact, different may mean the group is filtered by several categories in addition to those in the Global Group Profile. There are many ways a Group can be set up. The thing to remember is that a Group is set up to provide a different profile from the Global Group.

	Current Rules				-	
Group	Rule1 BYPASS *				New R	ule
	Rule # Rule1					Save
Joers						Save
	Rule Description BYPASS					
0 Users	Rule Details					
	Category	Pass	Allow	Warn	Block	Quote
	Category Groups	FBSO	mun	TYGETH	DECK	55008
	B Category Groups	0				
	Bandwidh	8				
	R Dainensitivestments	8				
	B Community/Organizations	ă				
	Education	8				
	R Containment	ě.				
	Government Law Politics	ă				
	e 🔁 Heath Finess	ő			-	
	B D llegal/Questionable	õ				
	19 Differention Technology	Ö	2			
	Internet Communication	ð				
	E C Internet Productivity	ő				
	19 internet/Intranet Mise.	Ö	2			
	E 🖸 News/Reports	Ó				
	🗄 🔂 Religion/Beliefs	Ô.				
	(# 🙆 Security	0				
	(E) 🔁 Shopping	0				
	E Society/Lifestyles	Ő				
	🖲 🛅 TravelEventa	0	1			
	E Custom Categories					

Rules window

The Rules window displays when Rules is selected from the Global Group menu. This window is used for adding a filtering rule when creating a filtering profile for an entity. By default, Rule 1 BYPASS displays in the Current Rules pull-down menu. The other choices in this pull-down menu are Rule 2 BLOCK Porn, Rule 3 Block IM and Porn, Rule4 M86 CIPA Compliance (which pertains to the Children's Internet Protection Act) and the Block All rule. By default, Rule 1 displays in the Rule # field, BYPASS displays in the Rule Description field, and Uncategorized Sites are allowed to pass.



NOTE: Uncategorized sites are those sited which have not been identified and placed within one of the 100+ categories in the Web Filter's Library database. The Pass default will allow those URLs to be viewed. Block will prevent those sites from being viewed.

How to create a new Rule

- 1. From the top level administrator console, select POLICY.
- 2. Click Global Group and select Rules.
- 3. In the Rule Details frame click **New Rule** to populate the **Rule #** field with the next consecutive rule number available.
- 4. Enter a unique **Rule Description** that describes the theme for that Rule.
- 5. By default, all library categories are included in the Pass Categories column. All categories are grouped in logical Category Groups. For example, in the Adult Content category group you would find the categories Child Pornography, Explicit Art, Obscene and Tasteless, R-Rated, and Pornography. To move all categories within a category group to another column, select the column next to the category group. To move a single category, expand the category group, and select the column for just that category.
 - Double click the Block column to move the library category to the blocked categories column.
 - Double click the Allow column to move the library category to the always allowed column.
- 6. Select Pass, Warn, or Block to specify whether all **Uncategorized Sites** should pass, warn the user, or be blocked.
- 7. Click **Save Rule** to include your Rule to the list that displays in the pull-down menu.

Global Group Profile

y : Global Group : C	ategory Profile 😡				15	2010/06/25.05
kçy 👘	Category Port Default Redirect URL Filter Options					
Global Group	Group: Global Group Current Profile: Custom Profile					
P						
1000 H	Available Filter Levels					
AlUsers	Custon Profile 💌					
	Rule Details					
	Category	Pass	Allow	Warn	Block	Quota
	Category Groups	- 13	8 8	6		
	🖸 🧰 Adult Content				0	
	🖲 🙆 Bandwidth					
	🗉 🚞 Business/Investments	0				
	E Community/Organizations	0				1
	🖲 🛄 Education	0				
	🗉 🚞 Entertainment	9	8			
	E Covernment/Law/Politics	0				1
	Heath/Fitness					
	🕀 🏠 liegal Guestionable	0			and the second sec	
	Information Technology	Q)		-		
	E Communication	0				
	🕀 🏠 Internet Productivity	0				
	🗷 🛅 Internet/Intranet Misc.					
	E C NewsReports	0				
	Relgion Belets	0				
	🖲 🚞 Security					
	🕀 🔂 Shopping	0				
	🗐 🏠 Society/Lifestyles	0				
	🕑 🚞 Travel/Events		-			
	E Custom Categories	0				
	Uncategorized Sites Pass 💌				Overall	0 <u>*</u> 110 ebuc
						[

Global Group Profile Category tab

The Global Group Profile window displays when Global Group Profile is selected from the Global Group menu.

Set the Global Group Profile

The Category Profile displays by default when Global Group Profile is selected from the Global Group menu. This window is used for selecting library categories that will be passed, warned, always allowed or blocked for the Global Group Profile.

By default, Custom Profile displays in the Available Filter Levels pull-down menu, and **Uncategorized Sites** are allowed to pass.

Create, edit a list of selected Categories

To define which categories will be passed, warned, always allowed or blocked in the Global Group Profile:

- 1. Select a library category from the Pass categories column.
- 2. Click in the appropriate column:
 - Double click the Block column to move the library category to the blocked categories column.
 - To remove a library category from the Block column, double click the Pass column.
 - Double click the Allow column to move the library category to the always allowed column.
- 3. Choose Pass, Warn or Block to specify whether **Uncategorized Sites** should pass, warn the user, or be blocked.

4. Click **Apply** to save the settings.

Group Profile

Review IRL Piter Optiona Review IRL Piter Optiona Review IRL Piter Optiona Review IRL Piter Level Svalible Filter Levels Curton Profile Y					義 臣 2010/06/25 09
roup: AllUsers Current Profile: Minimum l'illering Level Ivailable Filter Levels					
vailable Filter Levels					
					Minimum Filtering L
Custom Profile					Child Pornography
					Pornography/Adult Conten
Rule Details					
Category	Pass	Alicow	Warn	Block	Quota
	- //	8			
	<u>0</u>				
	Q			-	
	<u> </u>	-			
	<u>×</u>				
	X	-		-	·
		-			
	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	-			
	X	-		-	
				-	
	X	-			
	X			-	
	ă		_	-	
	ă				
	<u>8</u>	-			
			_		
	ŏ	-			
	Ő				
and the part of the part o		Category         Pasts           Category (roug)	Category         Pass         Abov           Category Orosos	Category     Pates     Allow     Warn       Category Orocs	Category     Parts     Allow     Warn     Block       Category Orocs

Group Profile window, Category Profile tab

The Group Profile window displays when Group Profile is selected from an IP Group.

## Set the Group Profile

Setting up a Group Profile is exactly the same as setting up the Global Group Profile, except that Rules can be used to define the Profile.

Category Profile displays by default when Group Profile is selected from an IP Group. This tab is used for selecting library categories that will be passed, warned, always allowed or blocked for the Group filtering profile.

By default, Rule0 Minimum Filtering Level displays in the Available Filter Levels pull-down menu, and Uncategorized Sites are allowed to pass.

To set the Profile of the Group, the administrator can either select a pre-set Rule or go through the process of moving library categories into the Pass, Allow, Warn or Block fields—or use both Rules and library Category selections to create a unique profile.

Selecting the library categories to be in the Pass, Allow, Warn or Block columns is just like configuring the Global Group Profile library Categories.

## Create, edit a list of selected Categories for a Group Profile

To define which categories will be passed, warned, always allowed or blocked in the Global Group Profile:

- 1. Select a library category from the Pass categories column.
- 2. Click in the appropriate column:
  - Double click the Block column to move the library category to the blocked categories column.
  - To remove a library category from the blocked categories column, double click the Pass categories column.
  - Double click the Allow column to move the library category to the always allowed column.
  - To remove a library category from the always allowed column, double click the Pass column to move that category back to the pass categories column.
- 3. Choose Pass, Warn or Block to specify whether **Uncategorized Sites** should pass, warn the user, or be blocked.
- 4. Click **Apply** to save the settings.

## **Group settings tests**

## Test the Rules and Profiles feature

To test the Rules and Profiles feature, first define a Rule.

obal Group : Au					(23)	2010/06/25 1
bal Group	Current Rules				New B	ule Delete
	Rule1 BVPASS					
logo AllUsers AP	Rule # Rule6					Save F
AlUsers						
A.P	Rule Description					
	Rule Details					
	Category	Pass	Allow	Warn	Block	Queta
	Category Groups				-	
	🗄 🛅 Adut Content				۲	
	🗄 🔂 Bandwidth	Ø				
	8 Business/Investments					
	B Community/Organizations	ð				
	🕀 🔂 Education	ő				
	🖲 Ertertainment	0				
	B Government Law Politics	ð				
	🗄 🛅 HealthFitness	0				
	🛞 🎦 llegal/Cuestionable	0				
	🖲 🛅 Information Technology	0	1			
	🗉 🧰 Internet Communication					10
	🛞 😋 Internet Productivity	0				
	🖲 🦳 Internet/Intranet Misc.	0	1			
	NewsReports	0				
	🗄 🔂 Religion/Beliets	Ő				
	🖲 🧰 Security	0	1			
	(E) Chopping	0				
	🗄 🔂 Society/Lifestyles	Ø				
	🖲 🧰 TravelEventa	0	1			
	E Custom Categories					

Rules window

- 1. Select **Rules** under Global Groups.
- 2. Click **New Rule** (the Rule # will reflect the next sequential number available for a rule).
- 3. Move categories from Pass categories to Allow, or Block as desired. Leave categories that don't need to be blocked in Pass.

**NOTE**: For the purposes of the evaluation, it is recommended that you only place two categories in Block and Allow. Leave the remainder in Pass.

- 4. Specify whether **Uncategorized Sites** should pass or be blocked.
- 5. Give the Rule a Description/Name.
- 6. Click Save Rule.
- 7. Select Yes when asked if you want to add the Rule.

## Test the Rule

To test the Rule, apply it to an IP Group.

	Alow	Wars	0	inimum Filte hid Pernography anography/Adut Quote
	Allow	Warn .	Block	hild Pornography ornography/Adul
	Alow	Warn .	Block	hild Pornography ornography/Adul
	Alow	Warn (	Block	hild Pornography ornography/Adul
	Allow	3Warn (	Block	ornography/Adul
Anss	Alow	3Vian (		Quota
	Allow	Warn (		Quote
000000000000000000000000000000000000000			۵	
000000000000000000000000000000000000000			0	
000000000000000000000000000000000000000				
000000000000000000000000000000000000000				
0000	_			
8				
8				
0				
0				
0				
0				
0				
0				
0				
0				
0				
0				
0				
9				
0				
	000000000000000000000000000000000000000	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	00000000	Correct Correct

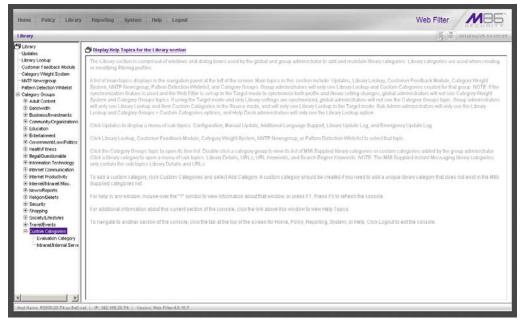
IP group profile window with rule applied

- 1. Select AllUsers from the IP Groups.
- 2. Select Group Profile.
- 3. In the Available Filter Levels field, select the Rule you created.
- 4. Click **Apply** in the bottom right corner.
- 5. Access the Internet from an IP address within the Sales group.
- 6. Attempt to access a Web site obviously included within the blocked categories contained in the Rule. The site will be blocked.
- 7. Access the Internet via an IP address *not* included in the Sales range and attempt to access the same URLs. Access *will not* be blocked.
- 8. Repeat with several Web sites and different categories, if desired.

## **Custom Categories**

## Create and configure a Custom Category

**Description**: The Web Filter allows an administrator to create a new category not listed among the 100+ options in the Library Categories. With literally tens of millions of URLs researched and screened among those existing categories, it might seem like a case of overkill to create a new one, but many of the most useful and powerful features of the Web Filter depend on the creation of Custom Categories.



Custom Categories in Library tree menu

## How to create a Custom Category

- 1. Navigate the top level administrator console to LIBRARY.
- 2. Click Custom Categories and select Add Category.
- 3. Provide a name and description for your custom category.
- 4. For evaluation purposes, call the new category Evaluation Category.
- 5. Add a Short Name description (7 characters maximum) and click Apply.

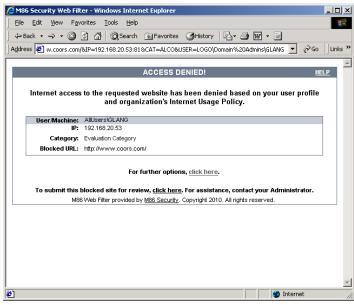
#### How to add URLs to the Custom Category

- 1. Select the newly created Custom Category.
- 2. Select the **URLs** option. The Web Filter provides the interface to add and remove sites from the custom category.
- 3. Type in a URL you want to add.

- Click Add. Wait for a moment while the Web Filter searches through all URLs in its Library database (including IP addresses) to find URL and IP matches. Matches are listed in the window.
- 5. Select all URLs and IP addresses you want to add from the list (use Ctrl and Shift keys to allow multiple selects).
- 6. Click Apply Action.
- 7. Repeat for each URL.

#### Custom Category setup and usage test

- 1. Create a custom category called Evaluation Category.
- 2. Add any three URLs per the previous configuration instructions.
- 3. Select **POLICY** from the top level administrator navigation.
- 4. Click Global Group and select Global Group Profile.
- 5. In the Category Profile tab, from the Pass column, select the Evaluation Category custom category you created and move it to the Block column.
- 6. Move any other category in the Block column to the Pass column.
- 7. Select Pass from Uncategorized Sites.
- 8. From an IP address contained within the Global Group range, attempt to access any of the URLs included in the Evaluation Category. Access is blocked.
- 9. Attempt to access a URL not in the Evaluation Category. Access is allowed.

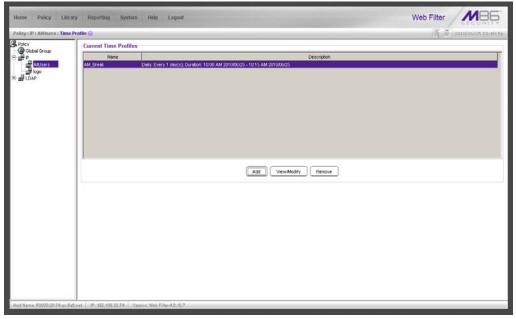


Block page

## Filtering profile features

## Time Profile feature

**Description**: The Time Profile feature lets the administrator set up a profile for any user or group to run at a scheduled time period. A user or group can have multiple time profiles, and these can be set to run at various intervals of time throughout a day, week, month, or year.



Time Profile window

## Set up a Time Profile

- 1. Select **POLICY** from the top level administrator console.
- 2. Choose AllUsers from the IP Groups, and select Time Profile from the menu.
- 3. Click Add, enter a name for the Time Profile, and then click OK.
- 4. Notice that the **Start** time is pre-populated with the closest 15-minute time period and the **End** time period is pre-populated with the time period an hour after the Start time. For the purpose of this exercise, change the End time to be 15 minutes after the Start time.

	e duration time	End: 03:30 - PM - 09/24/09
		Did. 0330 - Pm - 0502405
Recurrence C Daily	Every 1 day(s)	
C Weekly	every Ir any(s)	
C Monthly		
C Yearly		
	Start: 09/24/09 -	C End by: 09/24/09

Adding Time Profile window

- 5. Click the Rule tab.
- 6. Double click the **Society/Lifestyles** Category to open it.
- 7. Find Alcohol, double click in the **Block** column, and click **OK**.

**NOTE**: In order to perform the test that follows, be sure the Alcohol category isn't blocked in any other profile for this group.

- 8. Click **Apply** in the bottom right corner, click **Yes**, and then click **OK**.
- 9. Click Close.

#### **Test the Time Profile**

- From an IP address within the Sales group, access countless alcohol-related Web sites on the Internet for a 15-minute period—coors.com, absolut.com, budweiser.com, wine.com, etc. You should receive a block page when attempting to access these pages.
- 2. After the 15-minute period has ended, attempt to access URLs in the Alcohol category; you should be able to access these pages.

## Quota feature

**Description**: The Quota feature restricts the amount of time a user can spend in a passed category. When the user reaches 75 percent of time in a quota-designated category, the quota notice page pops up to warn the user about this information. If 100 percent of quota time is attained, the user receives a quota block page and cannot access that category until quotas are reset.



**NOTE**: If the Overall Quota is specified in the profile, the user's total quota time for all quota-marked categories is capped by the number of minutes entered in the Minutes field.

IP: Alliners: Cat	Profile O					\$ \$ 2010/06/25 10
	egory Frome M				12	Eller Lanningers ro
Potcy Color Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Potcy Po	Citegory Redirect URL   Fiter Options   Groux: AUSters: Current Profile: Custom Profile Available Filter Levels Custom Profile					Minimum Filtering L Child Pernography Pernography/Adult Corber
	Category	Pass	Allow	Warn	Block	Queta
	Category Groups	P303	Maure	37005	ORA	SACE
	E Category Groups					
	R Bandwith	0				
	Dusiness/Investments	ă				
	E Community/Organizations	ă				
	Education	ő				
	E Contertainment	ð	1			
	Covernment/Law/Politics	Ő				
	Heath/Fitness	0				
	🕀 🧿 Ilegal/Guestionable	0				
	Ca Information Technology	0	-			
	E 📸 Internet Communication	0				
	🕀 🏠 Internet Productivity	0				
	🗷 🛄 Internet/Intranet Misc.	Q)				
	E O NewsReports	0				•
	-      News	9				
	1. Sports	Q				5
	Westher/Traffic	<u>0</u>				
	🗄 🦳 World Cup	0		· · · · · · · · · · · · · · · · · · ·		
	Reigion/Delets	<u> </u>	1			
	B C Security	<u> </u>				
	R D Shopping	0				
	🗇 🦰 Societul itestules					
	Uncategorized Sites Pass 💌				Over	0 V 110 ebuD le

Quota time shown in Quota column and Overall Quota enabled

## Set up the Quota feature

- 1. Select **POLICY** from the top level administrator console.
- 2. Choose AllUsers from the IP Groups.
- 3. Double click the News/Reports Category to open it.
- 4. Find Sports, double click in the Quota column, and enter 5.
- 5. Click **Apply** in the bottom right corner.

#### Test the Quota feature

- From an IP address within the Sales group, access countless sports-related Web sites on the Internet for a five-minute period—espn.com, sportsillustrated.cnn.com, tennis.com, soccer.com, etc. During the course of the five minute period, you should receive a Quota Notice page informing you that 75 percent of quota time has been attained.
- 2. Continue accessing sports-related Web sites. After the five-minute period has elapsed, you should receive the Quota Block page informing you that your access to the Sports Category is now blocked.

Home Policy Library	Reporting System Help Logest	Web Filter
System : Quota Setting 😡		[] (元) 2010/06/25 10:54127
System     -Cortod     -Cortod     -Cortod     Admetation     Admetation     Admetation     Admetation     -Degrame     Degrame     D	Details         10           Seconds Per HL         10           Centralize Hits on Source:         III           Quala Reset         IIII           Current Reset Text(s)         IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Resol Now Remove New Resol Time (H4100) [2 ] : 00 ] Add
-SAM Hardwer Fakure Detecton -X Sirkes Blocking -Varin rigitori Setting -Outforceton -Sature Setting -Sature Setting -Sature Setting -Sature Setting		
<u>د ا</u>	et IP. 102.108.20.74 Venion: Web Filter 4.0.10.7	Apply

Quota Setting window

- 3. To reset the quota for your profile, first select **SYSTEM** from the top level administrator console.
- 4. Next choose Quota Setting.
- 5. Click **Reset Now** and then click **Apply**.
- 6. Using the same IP in the Sales group, attempt to access sports-related sites; you should be able to access these URLs again.

## White List feature

**Description**: White lists are effective when a particular group requires tight control over content options. For example, rather than spend hours determining what employees in shipping shouldn't be viewing, it is much easier to define only the things they *can* view. Restricting that group to specific URLs provides a way to ensure the only Web sites visited are those required for work—without requiring administrators to keep up with employees who find creative ways to bypass black lists.

e Policy Libr	ary Reporting System Help Logost				Web Filte	/ BEOUR	RIT
e: Global Group : Cate	egory Profile 😥				溪	2010/06/25 1	11:13
cy Global Group IP LOAP	Category [Port] Denual Redirect URL   Filter Options] Group: Global Group: Current Profile:Curton Profile Available Filter Levels Custon Profile *						
	Category	Pass	Allow	Warn	Block	Queta	-
	Adult Content	79835	eaure	37003	0000	GOOR	2
	E 🛅 Bandwidth				۲		
	Business/Investments		1		۲		
	Community/Organizations				۲		
	🗄 🚞 Education				۲		
	🕀 🔂 Entertainment				۲		
	CovernmentLawPolitics				۲		
	🕑 🚞 Heath/Fitness				۲		
	E C Regal/Guestionable				۲		
	Compation Technology				۲		
	P C Internet Communication				۲		
	🗄 🛄 Internet Productivity		2		8		
	🖲 🚞 Internet/Intranet Miss.						
	🕀 🏠 News/Reports				00000		
	🖲 🚞 Relgion@ellets		2		۲		
	🖲 🗀 Security				۲		
	🕀 🛄 Shopping				Q		
	🗄 🛄 Society/Lifestyles		2		۲		
	E 💭 Travel/Events				۲		
	🖂 🔁 Custon Categories						
	Evaluation Category		-				
	🕂 🔍 IntraneUnternal Servers	and the second se	-				
	-   White Lists		0	8		1	
	Uncategorized Sites Block 💌				Overall (	0 👻 110 ebud	٨
							Appl

White list rule setup

## How to create and configure a White List

- 1. Create a custom category called White Lists.
- 2. Add a couple of URLs that students might access for reference.
- 3. Select **POLICY** from the top level administrator navigation.
- 4. Click Global Group and select Global Group Profile.
- 5. In the Category Profile tab, select the White Lists custom category you created from the Pass categories column. Double click the Allow column.
- 6. Block all other categories by double clicking the Block column.
- 7. Select Block from Uncategorized Sites pull-down menu.
- 8. Click Apply.

#### **Test the White List**

After completing steps 1-8 above, then:

- 1. From an IP address contained within the Global Group range, attempt to access any of the URLs included in the Evaluation Category. Access is allowed.
- 2. Attempt to access a URL not in the White Lists category. Access is denied.

## Warn feature

The Warn feature allows the administrator to warn a user that sites within a specific category may violate the acceptable use policy, without actually blocking them from the site outright. The user will be prompted with a warning about the possibility of AUP violation. If the visit to the site is for appropriate business use, the user can elect to continue on to the site. If the user feels that they should not continue on to the site, they can also elect to do this.

#### How to test the Warn feature

- 1. Select the category you wish to Warn.
- 2. Double click the Warn column next to that category.
- 3. Visit that category on a filtered PC.

## Google/Bing/Yahoo!/Youtube/Ask/AOL Safe Search Enforcement

**Description**: Google, Bing, Yahoo!, YouTube, Ask, and AOL have very effective safe search features that can be activated to ensure search results do not contain sexually explicit material. Unfortunately, safe search can be deactivated in the preference settings of each search engine. The Web Filter allows these filters to stay activated—with the settings remaining unchangeable except by the administrator of the Web Filter.

Home Policy Libr	ary Reporting System Help Logost	Web Filter
Policy : Global Group : Filte	r Options 🚱	(A) (B) 2010/06/25 11/21/24
C Polcy C C C C C C C C C C C C C C C C C C C	Category   Port   befault Restrict URL   Filter Options   Filter Options X Striken Blocking Ø Google/Brg/midout/sub.files/LACL Safe Search Entrocement Search Engine Keywood Filter Control URL Reywood Filter Control Etitend URL Keyword Filter Control	
		Apply
Hort Name: R3000-20-74.go.84	0.rel   IP. 192.108.20.74   Vestion: Web Filter 4.0.10.7	

Safe Search Enforcement Filter Options

#### How to configure the Safe Search Enforcement feature

- 1. Select **POLICY** from the top level administrator console.
- 2. Click Global Group and select Global Group Profile.
- 3. Select the Filter Options tab.
- 4. Select the Google/Bing/Yahoo!/Youtube/Ask/AOL Safe Search Enforcement checkbox.
- 5. Click **Apply**.

#### How to test the Safe Search Enforcement feature

- 1. Configure the Google/Bing/Yahoo!/Youtube/Ask/AOL Safe Search Enforcement feature.
- 2. Access Yahoo! from an IP address within the Global Group range.
- 3. Manually set the Yahoo! search settings to the lowest filtering option.
- 4. Search using the term playboy. Content is filtered by Yahoo!
- 5. Repeat for Google, Bing, YouTube, Ask, and AOL.

## Search Engine Keyword Filtering

**Description**: There are a number of words and phrases that clearly won't be used to find business-related content on the Web. With Search Engine Keyword Filtering administrators can stop a search before it even starts (to cause trouble). The Web Filter allows administrators to add words or phrases, up to 75 characters in length (alphanumeric), to shut down access to restricted content right at the point an employee clicks search. These words and phrases can be added either one at a time or by uploading a text file. Instead of questionable content and/or images, a block page appears.

Home Policy Library	Reporting System Help Logoit	Web Filter
Library : Category Groups : Ca	intom Categories : Evaluation Category : Search Engine Keywords 😥	(張) (是) 2010/06/25 12:09:05 ·
Library     -Updates     -Updates     -Usray Lookup     Customer Feedbock Module     -Category Weight System     -NNTP Newsgroup     Pattern Detection Whitelst     Category Groups     Graduit Content	Edit Search Keyword List Keyword <u>shds on pool</u> Add <u>Remove</u> View Search Keyword Addition/Deletion List Select List	
Bandwidtn     Bandwidtn     Businessithrestiments     Comentity/Organizations     Education     Education     Education     Foretrainment     ConvertmentsLawsPolitics     Biseat/Funess     Billegat/Ouestionable     Finformation Technology		
Internet Communication     Internet Productive     Internet Productive     Internet Nexaux     Intern	Upload Search Keywords File	View Lut
4 5000-20-74.go.840.r	et   19.192.105.20.74   Veslow, Web Filter 4.0.10.7	

Search Engine Keyword filtering

## How to configure Search Engine Keyword Filtering



**NOTE**: Search Engine Keyword Filtering must be activated as part of a custom category.

- 1. Select **LIBRARY** from the top level administrator console.
- 2. Create a Custom Category (or add Search Engine Keyword Filtering to an existing custom category).
- 3. Select the Custom Category and choose Search Engine Keywords.
- 4. Type in a keyword and click Add.
- 5. Repeat and follow screen prompts.
- 6. Select **POLICY** from the top level administrator console.
- 7. Click on Global Group and select Global Group Profile.
- 8. Click the Filter Options tab.
- 9. Activate the Search Engine Keyword Filter Control checkbox.
- 10. Click Apply.

Home Policy Library	Raporting System Help Logost	Web Filter
Literary: Category Graups : Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes Ubdes U	eddin Categories ( Ponkution Category ( Search Engine Keywords 🖗 Eddi Search Keyword List View Search Keyword Addition/Deletion List Select List Select List Shot's ON GOUL HOCKLY Machty DUCKS	2010/06/3513/10:10
	Upload Search Keywords File Upload Search Keywords Upload Matter	Vew Litt Recost
White Lists	et   19:192.100.2074   Veslee, Web Filter 4.0.107	

Adding Search Engine Keywords

#### How to test Search Engine Keyword Filtering

- 1. Create a custom category called Keyword Filtering, using the keywords playboy, sex and porn.
- 2. Activate Search Engine Keyword Filtering in the Global Group Profile.
- 3. In the Global Group Profile, select the Category tab.
- 4. Move the Keyword Filtering category setup selection from Pass to Block.
- 5. Click Apply.
- 6. Access Yahoo! from an IP address within the Global Group range.
- 7. Enter playboy into the search field and click search. The search will be blocked.
- 8. Repeat for sex and porn.
- 9. Test in Google, Bing, YouTube, Ask, and AOL as well.

## Attachment filtering

**Description**: Unchecked and unmanaged, the download of attachments can bring a network to its knees. The Web Filter's Attachment Filtering feature identifies the download of a file as soon as it's initiated, and blocks the download.

Home Policy Library	Reporting System Help Logout	Web Filter
Library : Category Groups : Ca	untam Categories : File Extensions : URL Keywords 🚱	(院)(帝) 2010/06/25 13(20(21)
Construction	Edit Keyword List Keyword Addhion/Deletion List Select List Meder List Meder List FR3 Warv VIAV FR4 FR4 S94	Renove
B) Heath Thats B) Heath Thats B) Heath Constrained B) Heath Con	Upload Master URL Keyword File	Keywords Reload
<u> </u>	vt.   19.102.108.20.74   Venien, Web Filter 40.10.7	

Attachment filtering setup in URL Keywords

#### How to configure attachment filtering

- 1. Select **LIBRARY** from the top level administrator navigation.
- 2. Add a custom category and call it File Extensions.
- 3. Select URL Keywords from the newly-created File Extensions custom category.
- 4. Add a file extension in the Keyword field and click Add. (When adding the file extensions, make sure you add them with the period before the keyword, e.g. type .mp3 in the keyword field, not mp3).

Keep adding until you have entered all the desired file extensions.

- 5. Click **Reload** to reload the library.
- 6. Select **POLICY** from the top level administrator navigation.
- 7. Click Global Group and select Global Group Profile.
- 8. Select the Filter Options tab.
- 9. Enable URL Keyword Filter Control and click Apply to save.
- 10. Select the Category tab. Add the File Extensions custom category (found in the Pass column) to the Block column.

ibrary Reporting System Help Logent	Web Filter
ter Options 😥	[5] 4 2010/06/25 13:22:20
Category   Reviews LBL, TREF Options   Filter Options X Striken Blooking Ø OccupieBlogh Introd Would Leik Aldek ACL, Safe Search Enforcement Search Engine Keyword Free Control Ø UBL, Keyword Free Control Ø Edend UBL, Keyword Free Control	
	Acciv
	ter Options [} Category   Rodrect URL   Filer Options   Filter Options X Strates Bocking Ø OccupieSing/1 and/outube/Ask/ACC Safe Search Enforcement Search Enforcement USearch Depter Keywood Filer Control Ø URL Keywond Filer Control

Attachment filtering setup in Filter Options tab

## How to test attachment filtering

- 1. Configure the File Extensions custom category.
- 2. Enable URL Keyword Filter Control in the Global Group Profile.
- 3. Access the Internet from an IP address within the Global Group range.
- 4. Go to a Web site with file downloads (mp3, shareware, movies, etc.).
- 5. Attempt to download a file. The attempt will be blocked.

## Wildcard filtering

**Description**: Online communities such as myspace.com continually add numerous sub-domains to house the profiles of their fast growing communities. Rather than manually adding each and every individual domain to the library on an ongoing basis, the Web Filter can accept a wildcard to block these types of sites more efficiently. For example, adding http://*.myspace.com (where the asterisk [*] is the wildcard indicator) to a customized category's URL list will ensure that anything on myspace.com will be blocked.



**IMPORTANT**: If a specific URL was added to a custom library category that is **not** set up to be blocked, and a separate wildcard entry containing a portion of that URL is added to a category that **is** set up to be blocked, the end user will be able to access the non-blocked URL but not any URLs containing text following the wildcard.

For example, if *http://www.cnn.com* is added to a category that is **not** set up to be blocked, and *.cnn.com is added to a category that **is** set up to be blocked, the end user **will** be able to access: *http://www.cnn.com* since it is a direct match, but **will not** be able to access *http://www.sports.cnn.com*, since direct URL entries take precedence over wildcard entries.

Home Policy Library	Reporting System Help Logest	Web Filter
Library : Category Groups : Ca	istom Categories : Anaheim Ducks HHL : URL s 😥	「売」(売) 2010/06/25 13(27)54
Cubrary - Updates - Library Lookup - Customer Feedback Module - Calegory Weight System - NITP Newsgroup Pattern Outpoton Whether	Acton   View   Edit URL List URL	
Peter Detector Withdest Peter Detector Withdest B-Calegory Oryanization B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B-Dadows B	Edit WildCard URL List URL Prhilocks.com Add Remove example : * afe.com	
	Select URL(-j) to apply action.	Appy Actor
<b>N</b>		Upload Wildcard Master Upload Master Reload Library
Host Name: 83000-20-74 go 8x0.n	et   IP. 192.109.20.74   Vession, Web Filter 4.0.10.7	

Wildcard filtering

#### How to configure wildcard filtering

- 1. Go to **LIBRARY** in the top level administrator navigation.
- 2. Click an existing custom category or create a new one.
- 3. Select URLs from that category to add the wildcard URL.
- 4. In the URL text field enter the site in the format of *.site.com and click Add.
- 5. Highlight the newly added wildcard URL and click **Apply Action**.
- 6. Continue with any other wildcards you want to add.
- 7. Click Reload Library for changes to take effect.

**TIP**: Wildcards are to be used for blocking only. They are not designed to be used for the exceptions function or the always allowed white listing function. The minimum number of levels that can be entered is three (*.yahoo.com) and the maximum number of levels is six (*.mail.attachments.message.yahoo.com).

## How to test wildcard filtering

- 1. Create a custom category called Wildcards.
- 2. Add the following URLs (or any three URLs) per the previous configuration instructions:
  - a. *.playboy.com
  - b. *.myspace.com
  - c. *.8e6.com
- 3. Select **POLICY** from the top level administration navigation.
- 4. Click Global Group and select Global Group Profile.
- 5. In the Category tab, move the Wildcards custom category you created from the Pass column to the Block column.
- 6. Select the Block option from Uncategorized Sites.
- 7. From an IP address contained within the Global Group range, go to Google.
- 8. Initiate a search for any of the domains (using keywords playboy, myspace, and 8e6. You should get numerous sub-domain choices to select.
- 9. Attempt to access a link from Google. Access is denied.

## Configure, test, block services

## Anonymous proxies

**Description**: Web-based anonymous proxy services provide a method to bypass Web filters. Administrators can block the **Web-Based Proxies/Anonymizer** library Category to keep employees away from sites that offer free anonymous proxy services. As a second layer of protection, the Web Filter also offers **Proxy Pattern Blocking**.

**Proxy Pattern Blocking** prevents users from bypassing the filter if they try to use (unencrypted) Web and client-based proxies. Therefore, if the site is not categorized as Web-Based/Anonymous Proxies, the Web Filter will still be able to block access to the site based on signature files in the M86 Database.

Home Policy Library	Reporting System Help Logent	Web Filter
System : Control : Filter 😡		(張) (亞) 2010/06/25 13:3114
System     Society     System     Society     Soc	Local Filtering Local Filtering VLAN Detection HTTP Filtering HTTPS:SSL Filtering HTTPS:SSL Filtering HTTPS:SSL Filtering HTTPS:SSL Filtering HTTPS:SSL Filtering HTTPS:SSL Filtering HTTPS:SSL Filtering	C None C Low C Modum C High C None C Low C Modum C High Forward lookup to validate qualified DHS C non C Off
1 N		Apply
Host Name: R3000-20-74.go 8x0.n	et IP. 192.108.20,74 Veuton: Web Filter 4.0.10.7	

Block anonymous proxies

#### How to configure anonymous proxies

- 1. Select **SYSTEM** from the top level administrator console.
- 2. Click Control and select Filter.
- 3. Turn the Pattern Blocking radio button On.
- 4. Select **POLICY** from the top level administrator console.
- 5. Click Global Group and select Global Group Profile.
- 6. Move the **Web Based/Anonymous Proxy** category from the Pass column to the Block column.
- 7. Click Apply.

#### How to test anonymous proxies

- 1. From an IP address in the Global Group range, go to http://proxy.org and click on Free Proxy Form.
- 2. Enter any URL and select GO. The request is routed through anonymous proxies and is blocked.

## The Web Filter blocks these proxy types using the Proxy Pattern Detection feature:

- PHPproxy form (unencrypted): v0.3 and 0.4
- CGIProxy HTTP/FTP proxy in a perl based CGI script (unencrypted) including CGI-redirects: v2.0.1 and 2.1beta6
- Perl based proxy module: v5.8 (backward compatible)
- Accelerator and Split Proxies: GWA v0.2.64 and higher
- Anonymous and Transparent Proxies (unencrypted) used in combination with PHP, CGI, Perl, Accelerator
- Hopster (HTTP Tunnel): v17
- GCD related proxies: UltraReach (web-based), UltraSurf v6.9 and FreeGate v6.0

## Block IM, P2P applications and streaming media

**Description**: The Web Filter provides Peer-to-Peer (P2P) and Instant Message (IM) blocking. Peer-to-Peer and Instant Messaging pose significant challenges to administrators due to the risks of content type that can be passed on via these tools (images and video), as well as the ease by which these enable malicious code and viruses to circumvent many networks. Additionally, sites that offer IPTV programming, streaming video, streaming radio Internet programming and other such streaming media create a tremendous demand for network resources and can severely impact network performance. In addition to blocking IM and P2P applications, the Web Filter also logs user attempts to run these applications through the Web Filter's Intelligent Footprint Technology (IFT). IFT blocks these applications based on the traffic patterns they generate.

Home Policy Library	Reporting System Help Logent	Web Filter
System : Control : Filter 😡		「「」」 () 2010/06/25 13:25:25
System System Strate Administrator Administrator Administrator Oligonatics Aleft Software Update Synchronization Mode AdderGalation	Local Filtering Local Filtering VLAN Detection HTTP Filtering HTTP Packet Spilling Detection	Pon Cott Con Port Con Port
BackupRestore Rest Radius Authentication Setting SMMP Hardware Falure Detection - X Strikes Blocking - Ware Option Setting	HTTPS/SSL Filtering HTTPS/SSL Filtering Level	C None C Low @ Modium C High Forward lookup to validate gualitied DNS
Outcomization Outcomization Outco Setting SSL Certificate	Service Control Patern Blocking	€ on C otr
		(Aret)
<u>د ا</u>		Apphy
Host Name: R3000-20-74.go @e0.n	et   IP. 192,109:20.74   Venion: Web Filter 4.0.10.7	

Block patterns

#### Configure IM, P2P, streaming media blocking

- 1. Select **SYSTEM** from the top level administrator console.
- 2. Click Control and select Filter.
- 3. Turn the Pattern Blocking radio button to On.
- 4. Select **POLICY** from the top level administrator console.
- 5. Click Global Group and select Global Group Profile.
- 6. Move the Chat, Instant Messaging, Internet Radio, Peer-to-Peer/Filesharing and Streaming Media, from the Pass column to the Block column.
- 7. Click Apply.

## How to test for IM

- 1. From an IP address in the Global Group range, activate an IM program such as Yahoo! IM or AIM.
- 2. Attempt to send an instant message to another user. The attempt is blocked.

### How to test for P2P

From an IP address in the Global Group range, attempt to access a P2P site such as Limewire.com. The attempt is blocked.

#### How to test for streaming media

- 1. From an IP address in the Global Group range, open a streaming media application like Real Audio or Microsoft Media Player.
- 2. If a stream is not automatically initiated, activate streaming media content. The attempt is blocked.

## **Real Time Probes and X-Strikes Blocking**

## Real Time Probes feature

**Description**: Real time probes allow an administrator to monitor an employee's Internet usage in real time to determine if that user is accessing appropriate Internet content. Reports generated by the probe can be emailed for further review. Using Real Time Probes, an administrator can even monitor for malicious code and spyware in real-time to quickly identify workstations that are currently infected.

	rary Reporting System Hulp Logost	Web Filter
Reporting : Real Time Pro	ber : Configuration 😧	[5] Z.j District in the second sec
Report Configuration Report Configuration 2018 Enve Protos — Shadow Log Formet	Contention [Insultingot] Login Accounts] Real take Instein: R. Con C. Cont Maissian Instein In Andreaded Smithmonity Maissian Riso Take In Maders Maissian Riso Take In Maders Maissian Riso Take In Maders	10 6 7 4 Web Filter Real Time Proder 7 Web Filter
	Curret WM8 M of PE	Real Time Probe Reports           Orent Inter Pro
Mult Name (\$2000-20-74 st.)	(ut. not.   19, 192, 192, 20,54.   Viennin Web Schure 6.0, 10.7	Recurrence Code Code Code Code Code Code Code Cod

Real Time Probe setup

#### How to configure Real Time Probes

- 1. Select **REPORTING** from the top level administrator console and choose Real Time Probe.
- 2. Enable Real Time Probes by selecting **On** and clicking **Save** to apply your setting.
- 3. Click the link Go to Real Time Probe Reports GUI (lower right corner).
- 4. Select the **Create** tab do the following:
  - a. Enter a display name for the report (e.g. Spyware Monitoring).
  - b. Select **Category** for the Search option.
  - c. Select a category to be monitored, using the pull-down menu directly below the Search Option (the category choices include custom categories, as well).
  - d. Enter an email address where completed reports will be sent (optional).
  - e. Select **Now** for the Start Date and Time (or set a future date and time).
  - f. Enter the Total Run Time in Minutes you would like the probe to run (e.g. 30).
- 5. Click **Apply** and **OK** to confirm the creation of the report.

## How to test Real Time Probes

- 1. Configure a Real Time Probe with the following criteria:
  - Maximum Probes to Run/Schedule Simultaneously: 10
  - Maximum Probes that can be Scheduled: 5
  - Maximum Run Time in Minutes: 60
  - Maximum Report Lifetime in Days: 7
  - Display Name: Sports
  - Search Option: Category
  - Category: Sports
  - Start Date & Time: Now
  - Total Run Time in Minutes: 5
- 2. Click Apply and OK.
- 3. Click the **View** tab to see the probe that you have just created. Its status should show that it's currently running. Highlight the probe and click **View** to see the report run in real time.
- 4. Access the Web from an IP address included in the Global Group range.
- 5. Begin to access sports-related Web sites and content (e.g., Sports Illustrated and ESPN).
- 6. All access to sports-related sites will be identified in this report.

## X-Strikes feature

**Description**: The X-Strikes feature is a very powerful administrator tool that enables both the lockdown of users engaged in severe policy violations, as well as, remote notification of the violations, as they occur. X-Strikes is designed to identify and terminate Internet access of users who are frequent violators of policy, e.g. exhibiting multiple attempts to access blocked sites over short periods of time.

Home Policy Librar	ry Reporting System Help Logost	Web Filter
Policy : Global Group : Filter	Options Q	張」 <u>優</u> 」 2010/06/25 13(47)14
Broov F@ Bood Group B and Group B ar Loup	Cotegory   Nori   Default Resterct URL   Titer Options   Filter Options V X Strikes Risoking Options/Philod/WorkdalAsk/ACL Safe Search Entropement V Seek: Depark Hayword Filter Cottrol URL Keyword Filter Cottrol Estend URL Keyword Filter Control	
		Apply
Host Name: 83000-20-74 go 845	0.net   IP. 192.100.20.74   Vestion: Web Filter 4.0.10.7	

X-Strikes feature

## How to configure the X-Strikes feature

There are two sections of the administrator console that must be accessed to configure the X-Strike feature. First, the feature must be activated in the Global Group options.

- 1 Select **POLICY** from the top level administrator console.
- 2 Select Global Group Profile from the Global Group.
- 3 Select the Filter Options tab in the Global Group window.
- 4 Select the X-Strikes Blocking checkbox.

Home Policy Library	Reporting System Help Logost	Web Filter
System : X Strikes Blocking : C	Configuration Q	(英) <b>基</b> ) 2010/06/25 13(49:52)
Control     Contro     Control     Control     Control     Control     Control     Co	Configuration   Email Alter   Logon Accounts   Categories   Reset the X-Strike court upon sutherstation C On @ Ott Maximum Strikes Before 1 onling" the Vorkstation Time Span in Minutes to Track the No. Strikes Within Category Flood Tolerance Delay Specify the "Locked" Life Time (Messured in Minutes): C Lifelined @ Defined © Defined "Atternato" Locked Block Page C Cution URL Reset All Strikes Utiliack All Locks	<u>р</u> 
<u> </u>		Go to X Strikes Unlock Workstation GU
Host Name: R3000-20-74.go 8x8.m	el IP. 192.108.20.74 Veulon, Web Filter 4.0.10.7	

X Strikes Blocking

Next, the actual parameters of the X-Strike feature need to be configured.

- 1. Select **SYSTEM** from the top level administrator console.
- 2. Click X Strikes Blocking.
- 3. Make the following settings:
  - a. Select **On** radio button to reset X-Strike Count upon authentication (resets counter for each new user).
  - b. Set Maximum Strikes Before Locking the Workstation. The number entered in this field determines how many time a user can attempt to access blocked content before that user is prevented from further Internet access. For example, if the threshold is set at 5, then on the user's fifth attempt to access blocked sites, the computer will be locked down—*if that attempt is made within the time threshold set in step 3b*. The lock disables further access and, instead only displays a block page indicating the reason that access has been blocked.
  - c. Set the **Time Span in Minutes to Track the No. Strikes Within Category**. The number entered in this field determines how long the strikes will be monitored to qualify for a lockdown. For example, if the threshold is set at 5 (minutes) and the Maximum Strikes threshold is set at 5 (attempts), a user who attempts to access five blocked sites being monitored by the X-Strikes feature in a five minute (or less) period of time will be locked out of the Internet and the administrator will be notified. However, if the user attempts to access five blocked sites over the course of an entire day, the standard block page will appear and Internet access will not be locked.
  - d. Set the Flood Tolerance Delay (in seconds) to determine the maximum delay that will occur before a user who accesses the same URL will receive another block page. If a user receives a block page and attempts to flood the filter through rapid refresh of the page, the X-Strikes feature will not log a strike for every attempt but instead log a strike for each Flood Tolerance Delay threshold that reached. For example, if an employee accesses a

blocked site monitored by X-Strikes (which is set at 3 strikes in 1 minute for lockdown), he receives a block page and X-Strikes logs one strike. If the Flood Tolerance Delay is set at 4 seconds, the employee keeps getting block pages, but won't be locked down until 12 seconds has elapsed—no matter how many times he tries to refresh the blocked site.

- e. Specify the Locked Life Time (Measured in Minutes) to determine how long Internet access will be denied.
- 4. Select the Email Alert tab, and make the following settings:
  - a. In the **Minutes Past Midnight Before Starting Time Interval** field, enter the number of minutes past midnight that a locked work station email alert will first be sent to the specified recipient(s).
  - b. In the **Interval Minutes to Wait Before Sending Alerts** field, enter the number of minutes within the 24-hour period that should elapse between email alerts. For example, by entering 300 in this field and 30 in the previous field, if there are any locked workstations, an email will be sent at 5:30 AM, 10:30 AM, 3:30 PM, 8:30 PM and 12:00 AM (the email alert at midnight fills the gap before the time interval is reset). To check the time(s) the email alert is scheduled to occur, click the Display Sending Time button to open the Daily Schedule pop up window in the (HH:MM:SS) format.
  - c. Click **Save** to save the settings.
  - d. In the **Email Address** field, enter the email address(es) of those who will receive locked workstation alerts.
  - e. Click Add to include them in the list.
- 5. Select the Categories tab.
- 6. Move the categories from the No Strike category you want monitored to the Strike Categories and vice versa.

Home Policy Library	Reporting System Help Logost	Web Filter
System : X Strikes Blocking :	Configuration Q	5 Di 2010/06/25 10:52:51
System     -Cortol     -Cortol     Administrator     Administrator     Administrator     Secure Logon     Diagnostics     Adet     Suthware Update     -Synchronization     Mode     -Mutantification     Boalup,Restore     Reset     Raduu Authorization Setting     -Staff     Indonare Failure Detection     Quicto setting     Outdon Setting     -Staff     Customization     Quicto setting     -Staff     Site Customization     Site Customization	Configuration   Email Aller   Logan Accounts   Categories   Reset the X-Strike court upon eutheritication @ On C Otr Maximum Strikes Extreme Tunking the Vibrishation Time Span in Minutes to Track the No. Strikes Wibin Category Flood Tolerance Delay Specify the Tunking Life Time (Measured in Minutes). C Unleaded @ Defined  2 Specify a Rindmot Life, @ Defined *Atemate* Locked Block Page C Custon URL Reset All Strikes Uklick All Looks	2 2 5 5000
I ≥ 1		Go to X Strikes Unlock Workstation GU
Host Name: R3000-20-74.go Be0.n	et   IP. 192.108.20.74   Vention: Web Filter 4.0.10.7	

X Strikes testing

## How to test X-Strikes

- 1. Set up X-Strikes with the following settings:
  - a. Configuration:
    - Reset X-Strike Count Upon Authentication: ON
    - Maximum Strikes Before Locking the Workstation: 3
    - Time Span in Minutes to Track the No. of Strikes Within The Category: 2
    - Flood Tolerance Delay: 2
    - Specify Locked Life Time: 2
    - Specify a Redirect URL: DEFAULT
    - Email Alert: enter your email address
    - Minutes Past Midnight Before Starting Time Interval: 0
    - Interval Minutes to Wait Before Sending Alerts: 1
    - Enter an email address to receive alerts; Click Add
  - b. Categories:
    - Strike Categories: Pornography/Adult Content
    - No Strike Categories: All others
- 2. Using an IP within the Global Group range, access www.playboy.com. The site should be blocked.
- Continue to refresh the page for approximately 6-8 seconds. The workstation's Internet access will be locked and a block page indicating he locked status will appear.
- 4. After 2 minutes, access will be available again.
- 5. In approximately 1-2 minutes (the nuances and security settings of the email server will impact the speed of delivery, as well) a notification should be received at the email address noted in the Email Alert field.

M86 Security Corporate Headquarters (USA): 828 West Taft Avenue Orange, CA 92865-4232 • Tel: 714.282.6111 or 888.786.7999 Fax: 714.282.6116 (Sales/Technical Support) • 714.282.6117 (General Office)