

GFI WebMonitor 2011 for ISA/TMG

GFI WebMonitor[™]

Administration and Configuration Manual



<http://www.gfi.com>
info@gfi.com

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical. All product and company names herein may be trademarks of their respective owners.

GFI WebMonitor is copyright of GFI SOFTWARE Ltd. - 1999-2011 GFI Software Ltd. All rights reserved.

Last updated: 12 September 2011
Version number: WEBMON-ISATMG-ACM-EN-2.1.1

Contents

1	Introduction	1
1.1	Who is This Manual For?	1
1.2	About This Manual.....	1
1.3	Terms Used in This Manual.....	2
2	Using the GFI WebMonitor Dashboard	3
2.1	Introduction	3
2.2	The GFI WebMonitor Dashboard.....	3
3	Monitoring Internet Activity	11
3.1	Introduction	11
3.2	Active Connections.....	11
3.3	Past Connections	12
3.4	Hidden Downloads.....	12
3.5	Search.....	14
3.6	Access Monitoring	15
3.7	Blocked Monitoring.....	18
4	Allowing and Blocking Users, IP Addresses and Sites	19
4.1	Introduction	19
4.2	Whitelist	19
4.3	Blacklist.....	21
4.4	Using Wildcards.....	22
5	WebFilter Edition - Site Rating and Content Filtering	23
5.1	Introduction	23
5.2	Web Browsing Policies	23
5.3	Web Browsing Thresholds	29
5.4	Web Filtering Policies.....	30
5.5	Configuring Advanced Web Filtering Policy Conditions	36
5.6	WebGrade Database	38
6	WebSecurity Edition - File Scanning and Download Control	41
6.1	Introduction	41
6.2	Download Control Policies	41
6.3	IM (Instant Messaging) Control Policies.....	47
6.4	Virus Scanning Policies	51
6.5	Virus & Spyware Protection.....	57
6.6	Anti-Phishing Engine	60
7	Configuring GFI WebMonitor	63
7.1	Introduction	63
7.2	Administrative Access Control.....	63
7.3	Anonymization	65
7.4	Notifications	66
7.5	General Settings	67

7.6	Reporting	71
7.7	Safe Search.....	75
8	Quarantine	77
8.1	Introduction	77
8.2	Viewing Quarantined Items	78
8.3	Approving Quarantined Items.....	79
8.4	Deleting Quarantined Items.....	79
9	Troubleshooting	81
9.1	Introduction	81
9.2	Knowledge Base	81
9.3	Web Forum	81
9.4	Request Technical Support.....	81
9.5	Build Notifications.....	81
10	Glossary	83
	Index	87

1 Introduction

GFI WebMonitor is a comprehensive monitoring solution that enables you to monitor and filter network users' web traffic (browsing and file downloads) in real-time. It also enables you to block web connections in progress as well as to scan traffic for viruses, trojans, spyware and phishing material.

It is the ideal solution to transparently and seamlessly exercise a substantial degree of control over your network users' browsing and downloading habits. At the same time, it enables you to ensure legal and best practice initiatives without alienating your network users.

1.1 Who is This Manual For?

This manual is for administrators who want to use GFI WebMonitor as a plug-in for Microsoft ISA Server or Microsoft Forefront TMG.

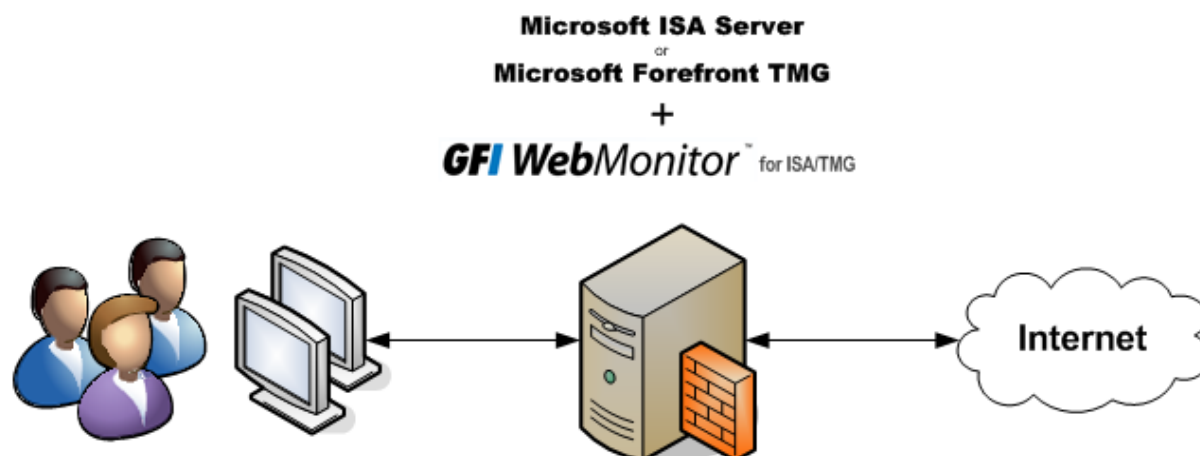


Figure 1 - GFI WebMonitor Environment

For environments where there is no Microsoft ISA Server or Microsoft Forefront TMG server, an independent version of GFI WebMonitor is available. For more information, refer to: <http://www.gfi.com/internet-monitoring-software/webmonfeatures.htm>.

1.2 About This Manual

The aim of this manual is to help you use and configure GFI WebMonitor on your network.

This manual is structured as follows:

CHAPTER	DESCRIPTION
Chapter 1	Introduction Introduces this manual.
Chapter 2	Using the GFI WebMonitor Dashboard Provides information on how to access and use GFI WebMonitor's dashboard.
Chapter 3	Monitoring Internet Activity Provides information on how to monitor Internet activity.
Chapter 4	Allowing and Blocking Users, IP Addresses and Sites Provides information on how to configure allowed and blocked entities.
Chapter 5	WebFilter Edition - Site Rating and Content Filtering Provides information on how to configure WebFilter Edition policies.

CHAPTER	DESCRIPTION
Chapter 6	WebSecurity Edition - File Scanning and Download Control Provides information on how to configure WebSecurity Edition policies.
Chapter 7	Configuring GFI WebMonitor Provides information on how to configure GFI WebMonitor settings.
Chapter 8	Quarantine Provides information on how to configure and manage quarantined items.
Chapter 9	Troubleshooting Provides all the necessary information on how to deal with any problems encountered while using GFI WebMonitor. Also provides extensive support information.
Chapter 10	Glossary Defines technical terms used within GFI WebMonitor.




Getting Started Guide

Detailed installation guidelines are provided in the **Getting Started Guide**, which is downloadable from the GFI website at <http://www.gfi.com/products/gfi-webmonitor/manual>

The Getting Started Guide provides detailed information on how to select your deployment environment and install GFI WebMonitor with default settings.

1.3 Terms Used in This Manual

The following terms are used in this manual:

TERM	DESCRIPTION
	Additional information and references essential for the operation of GFI WebMonitor.
	Important notifications and cautions regarding potential issues that are commonly encountered.
	Step by step navigational instructions to access a specific function.
Bold text	Items to select such as nodes, menu options or command buttons.
<i><Italics text></i>	Parameters and values that you must replace with the applicable value, such as custom paths and filenames.

For any technical terms and their definitions as used in this manual, refer to the **Glossary** chapter in this manual.

2 Using the GFI WebMonitor Dashboard

2.1 Introduction

The **Dashboard** node enables you to obtain graphical and statistical information related to the operation of GFI WebMonitor. This includes:

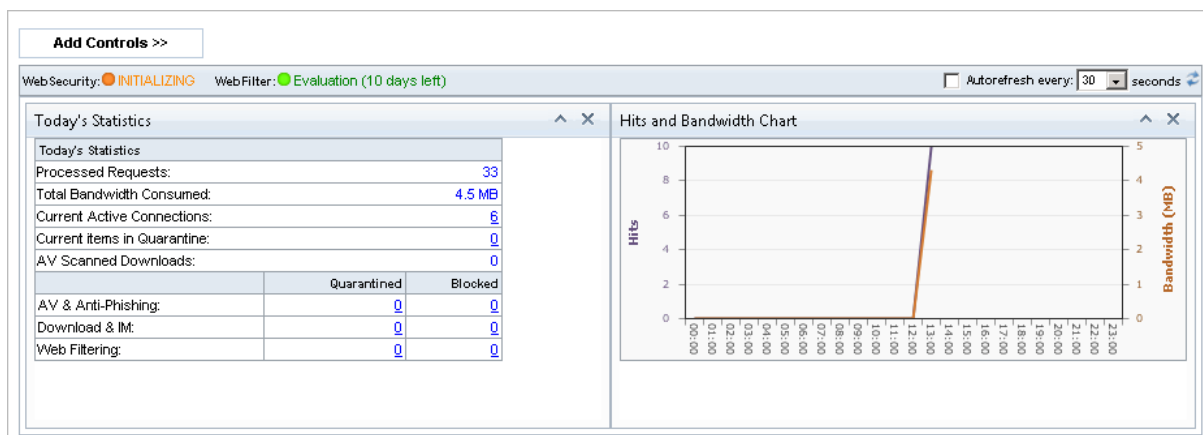
- » Usage and operations statistics
- » Hits over time and bandwidth usage trend charts
- » WebFilter statistics, Last blocked requests and security threats.



If Anonymization is enabled, personal data (such as User Names and IPs) will be masked. For more information refer to the [Anonymization](#) section in this manual.

2.2 The GFI WebMonitor Dashboard

The **Dashboard** node in the navigation bar provides access to the GFI WebMonitor Dashboard which is described in detail in the sections below.



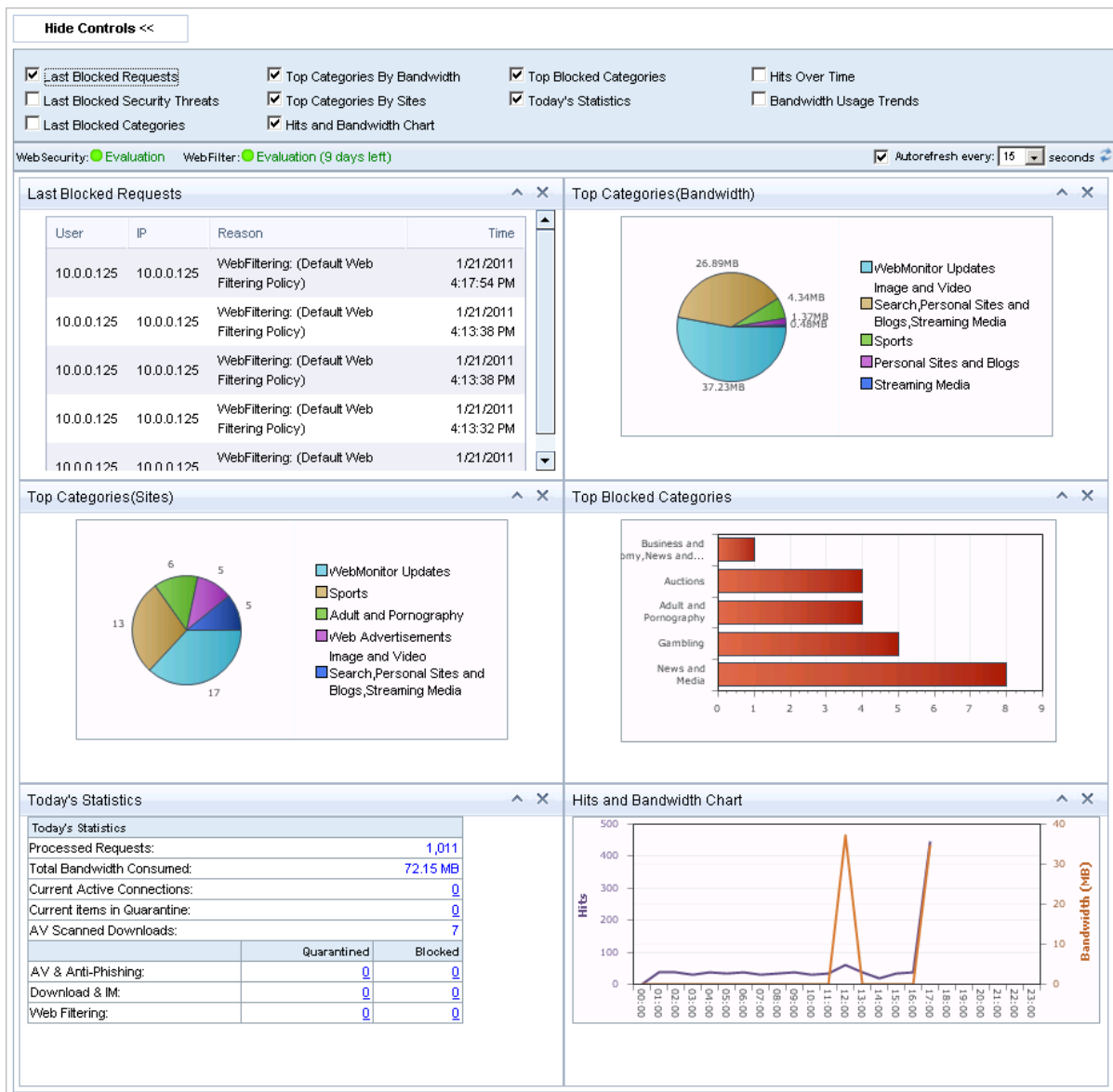
Screenshot 1 - Dashboard Default view

By default the view displays two windows:

- » Today's Statistics
- » Hits and Bandwidth Chart.



All graphical and statistical information within the **Dashboard** node displays browsing information for past dates and the current day (the current day is calculated from midnight to the instant the dashboard is launched).



Screenshot 2 - Dashboard expanded view


Click **Add Controls >>** to display a number of controls that enable you to customize the view. The available windows are:

- » Last Blocked Requests
- » Last Blocked Security Threats
- » Last Blocked Categories
- » Top Categories By Bandwidth
- » Top Categories By Sites
- » Hits and Bandwidth Chart
- » Top Blocked Categories
- » Today's Statistics
- » Hits Over Time
- » Bandwidth Usage Trends

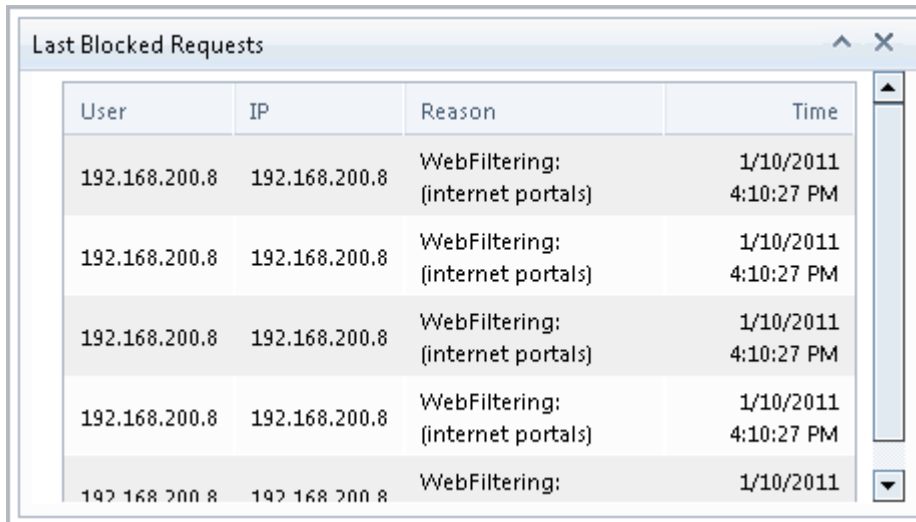
Once controls are added and the view is customized, GFI WebMonitor retains this view even when the application is closed. Windows within the view can be collapsed and moved about the

main window by holding down the left mouse button and dragging the window to the desired location.



Click refresh  at the upper right corner to refresh the displayed information.

Last Blocked Requests



User	IP	Reason	Time
192.168.200.8	192.168.200.8	WebFiltering: (internet portals)	1/10/2011 4:10:27 PM
192.168.200.8	192.168.200.8	WebFiltering: (internet portals)	1/10/2011 4:10:27 PM
192.168.200.8	192.168.200.8	WebFiltering: (internet portals)	1/10/2011 4:10:27 PM
192.168.200.8	192.168.200.8	WebFiltering: (internet portals)	1/10/2011 4:10:27 PM
192.168.200.8	192.168.200.8	WebFiltering: (internet portals)	1/10/2011

Screenshot 3 - Dashboard: Last Blocked Requests list

The **Last Blocked Requests** list displays the five most recent entries blocked for the current day. This enables you to identify problems with blocked requests regardless of whether these blocked requests are reported to you or not.

Last Blocked Security Threats

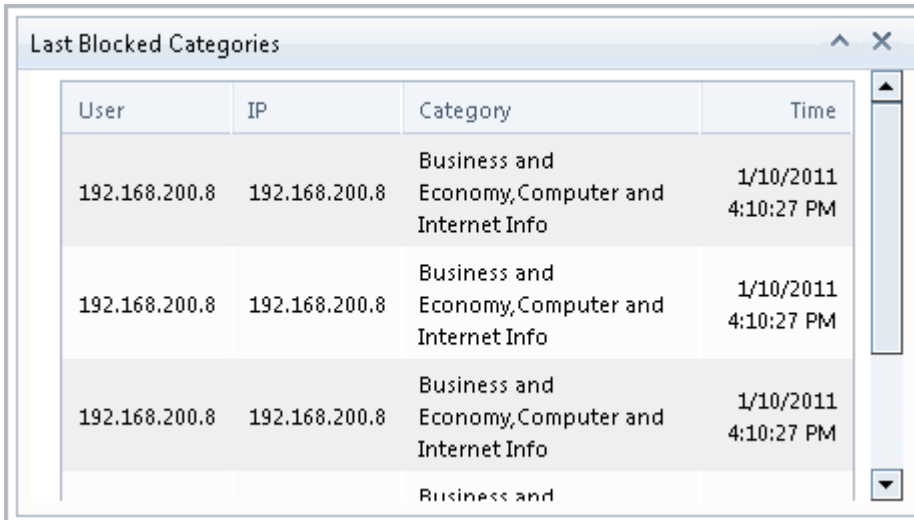


User	IP	Threat/Virus	Time
10.0.0.125	10.0.0.125	Scanned with Bitdefender Scanned with Norman Kaspersky: File could not be scanned. Password protected.	1/21/2011 4:17:12 PM
10.0.0.125	10.0.0.125	Bitdefender: Infected:WIn32.Novarg.A@mm Norman: Infected with MyDoom.A@mm Kaspersky: Infected:Email- Worm.WIn32.Mydoom.a	1/21/2011 4:17:07 PM

Screenshot 4 - Dashboard: Last Blocked Security Threats list

The **Last Blocked Security Threats** list displays the five most recent entries detected as threats/viruses for the current day. This enables you to identify security issues as early as possible, in time to take preventive measures before your network security is breached.

Last Blocked Categories

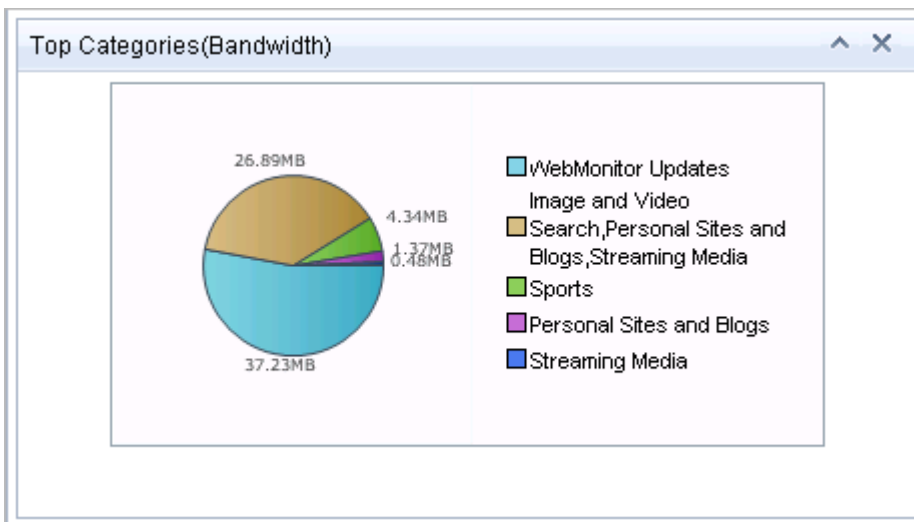


User	IP	Category	Time
192.168.200.8	192.168.200.8	Business and Economy, Computer and Internet Info	1/10/2011 4:10:27 PM
192.168.200.8	192.168.200.8	Business and Economy, Computer and Internet Info	1/10/2011 4:10:27 PM
192.168.200.8	192.168.200.8	Business and Economy, Computer and Internet Info	1/10/2011 4:10:27 PM

Screenshot 5 - Dashboard: Last Blocked Categories

The **Last Blocked Categories** list displays the five most recent entries blocked for the current day.

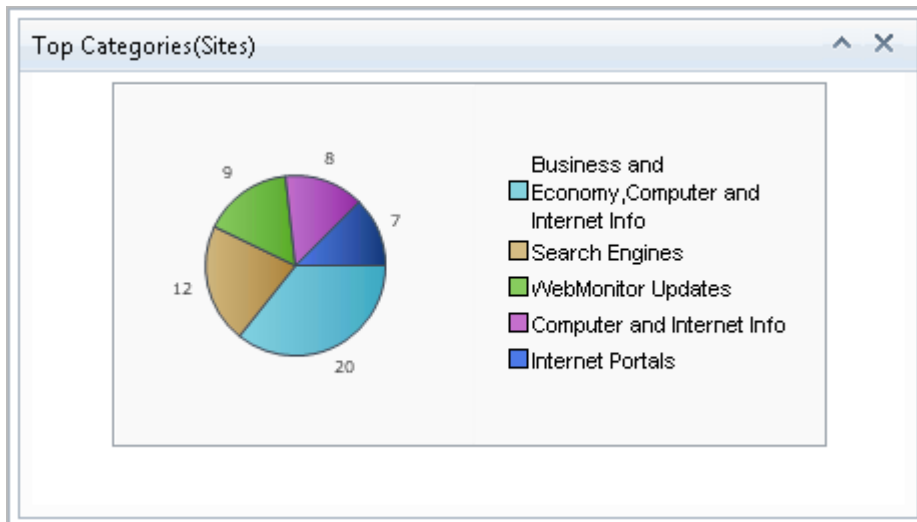
Top Categories (Bandwidth)



Screenshot 6 - Dashboard: Top Categories (Bandwidth) chart

The **Top Categories (Bandwidth)** chart is a graphical representation of the bandwidth use split by categories for the current day.

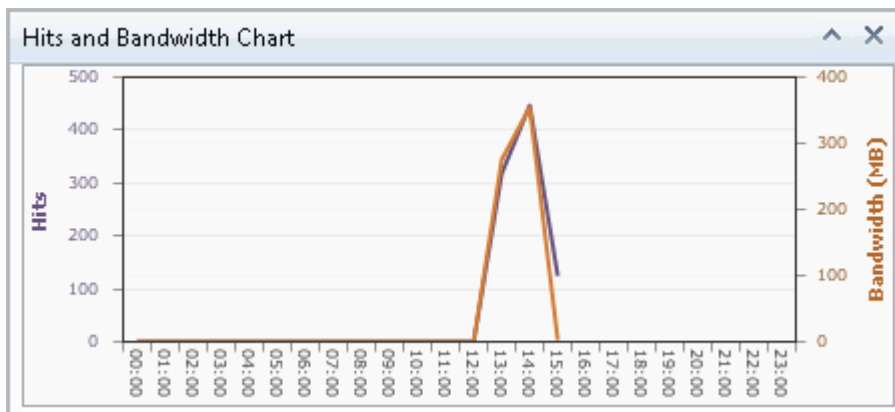
Top Categories (Sites)



Screenshot 7 - Dashboard: Top Categories (Sites) chart

The **Top Categories (Sites)** chart is a graphical representation of the top hits (HTTP requests) split by categories for the current day. This enables you to gain knowledge on site categories being visited by web users.

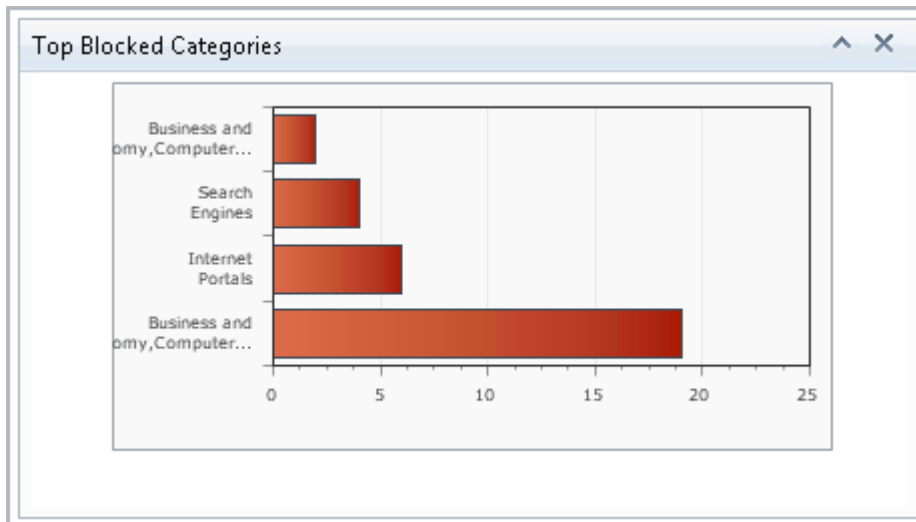
Hits and Bandwidth Chart



Screenshot 8 - Dashboard: Hits and Bandwidth Chart

The **Hits and Bandwidth Chart** enables you to view a graphical representation of the relationship between the number of hits and bandwidth use for the current day.

Top Blocked Categories (Hits) chart



Screenshot 9 - Dashboard: Top Blocked Categories (Hits) chart

The **Top Blocked Categories (Hits)** chart is a graphical representation of the blocked HTTP requests for the current day. This enables you to identify the main reasons of why requests were blocked.

The chart displays data only once policies are in place.

Today's Statistics

Today's Statistics		
Processed Requests:		439
Total Bandwidth Consumed:		606.64 MB
Current Active Connections:		3
Current items in Quarantine:		0
AV Scanned Downloads:		3
	Quarantined	Blocked
AV & Anti-Phishing:	0	0
Download & IM:	0	0
Web Filtering:	0	0

Screenshot 10 - Dashboard: Statistics

The information provided in the **Today's Statistics** table lists a number of important operational elements of GFI WebMonitor for the current day.

- › Click **Current Active Connections** to view information related to any user request that is being processed at the instant the report is launched or refreshed. This is also accessible from the **Monitoring** node.

For more information, refer to the **Active Connections** section in the Monitoring Internet activity chapter.

- › Click **Current items in Quarantine** to view a summary of the quarantine folder. This view can also be accessed from the **Quarantine** node.

For more information, refer to the [Viewing Quarantined Items](#) section in the Quarantine chapter.

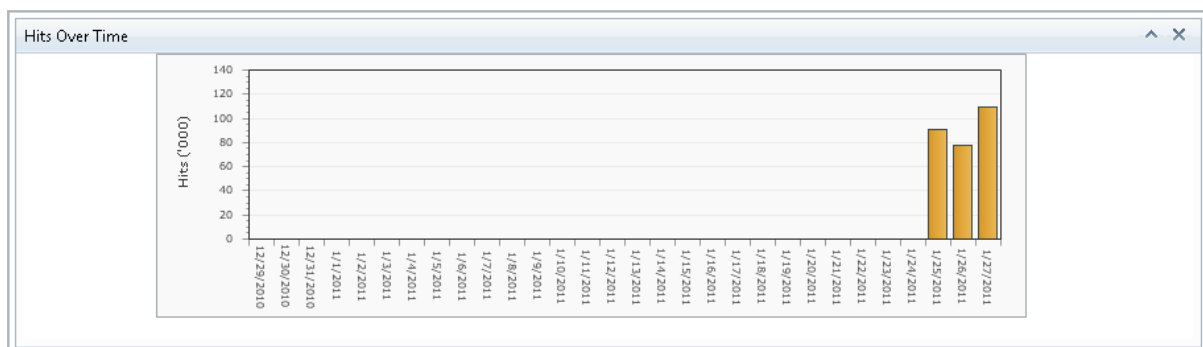
- » Click **AV Scanned Downloads** to view the total number of downloads scanned by the anti-virus engines.

For more information, refer to the section [Virus & Spyware Protection](#) in the WebSecurity Edition - File scanning and download control chapter.

- » Click the hyperlinks under the **Quarantined** and **Blocked** columns to view further detail on the statistics as summarized below:

FEATURE	QUARANTINED	BLOCKED
AV & Anti-Phishing	Select the hyperlink under Quarantined to approve or delete quarantined items in the Virus Scanning Policies category. For more information, refer to the Viewing Quarantined Items section.	Select the hyperlink under Blocked to view the Blocked Monitoring by Policy Report . For more information, refer to the Blocked Monitoring section.
Download & IM	Select the hyperlink under Quarantined to approve or delete quarantined items in the Download Control Policies category. For more information, refer to the Viewing Quarantined Items section.	Select the hyperlink under Blocked to view the Blocked Monitoring by Policy Report . For more information, refer to the Blocked Monitoring section.
Web Filtering	Select the hyperlink under Quarantined to approve or delete quarantined items in the Web Filtering Policies category. For more information, refer to the Viewing Quarantined Items section.	Select the hyperlink under Blocked to view the Blocked Monitoring by Policy Report . For more information, refer to the Blocked Monitoring section.

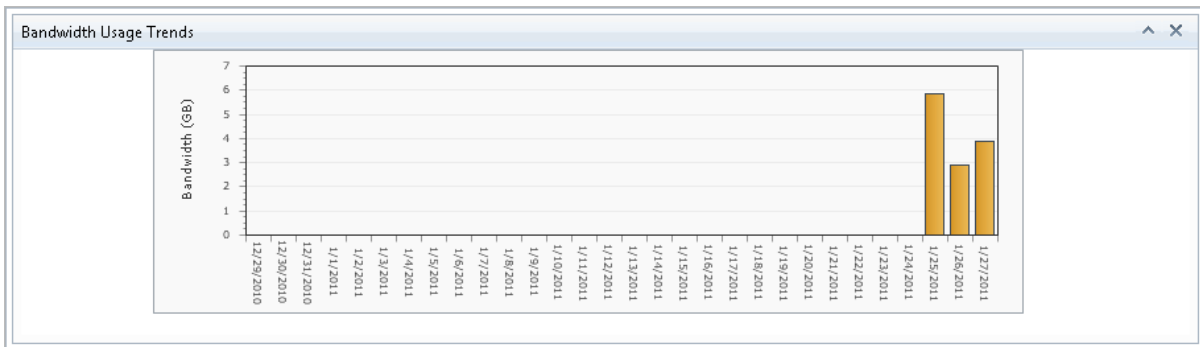
Hits Over Time chart



Screenshot 11 - Dashboard: Hits Over Time chart

The **Hits Over Time** chart is a graphical representation of the total number of hits per day over the last 30-day period, including the current day. This enables you to identify a pattern of how website hits fluctuate on a day-by-day basis and also helps to identify any anomalies.

Bandwidth Usage Trends chart



Screenshot 12 - Dashboard: Bandwidth Usage Trends chart

The **Bandwidth Usage Trends** chart is a graphical representation of the total bandwidth use per day over the last 30-day period and includes the current day. This enables you to identify patterns and trends of how bandwidth is utilized on a day-by-day basis and to identify spikes and anomalies.

3 Monitoring Internet Activity

3.1 Introduction

The **Monitoring** node and its sub-nodes enable you to examine current and historical web request data processed by GFI WebMonitor. Through these nodes, you can view data related to:

- » Active Connections
- » Past Connections
- » Hidden Downloads
- » Searches and reports
- » Access Monitoring
- » Blocked Monitoring



If Anonymization is enabled, personal data (such as User Names and IPs) will be masked. For more information refer to the [Anonymization](#) section in this manual.

3.2 Active Connections

The **Active Connections** report provides information related to current active connections.

User	IP	Bytes	Status	URL
tcdomaina.com/administrator	192.168.200.7	772,978	Receiving real filetype:pdf	http://www.gfi.com/webmon/webmonmanual.pdf
tcdomaina.com/administrator	192.168.200.7	808,858	Receiving real filetype:pdf	http://www.gfi.com/webmon/webmongsg.pdf

Screenshot 13 - Monitoring: Active Connections view

Navigate to **Monitoring ► Active Connections** to access the **Active Connections** view.

The information displayed includes:

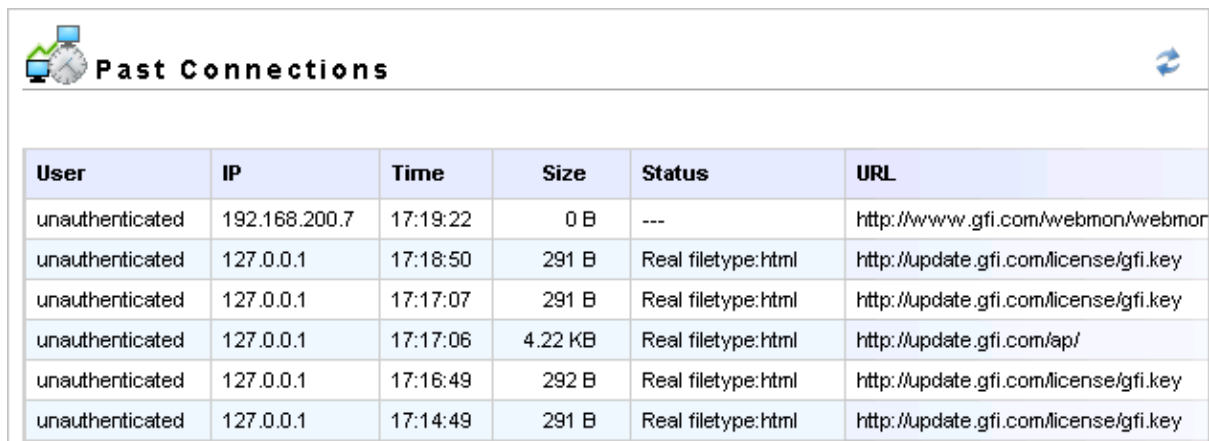
COLUMN	DESCRIPTION
User	The user being monitored and whose request is being processed at the instant the report is launched or refreshed
IP	The IP being monitored and whose request is being processed at the instant the report is launched or refreshed
Bytes	The size of the download at the instant the report is launched or refreshed
Status	The status of the connection (for example, Connecting or Receiving) at the instant the report is launched or refreshed
URL	The URL of the request that is currently being processed

Further Information

Click the button in the **Status** column of the related connection to terminate the download (for example, interrupt file downloads that are taking up too much bandwidth).

3.3 Past Connections

The **Past Connections** report shows the last 2000 complete connections processed by GFI WebMonitor.



User	IP	Time	Size	Status	URL
unauthenticated	192.168.200.7	17:19:22	0 B	---	http://www.gfi.com/webmon/webmor
unauthenticated	127.0.0.1	17:18:50	291 B	Real filetype:html	http://update.gfi.com/license/gfi.key
unauthenticated	127.0.0.1	17:17:07	291 B	Real filetype:html	http://update.gfi.com/license/gfi.key
unauthenticated	127.0.0.1	17:17:06	4.22 KB	Real filetype:html	http://update.gfi.com/ap/
unauthenticated	127.0.0.1	17:16:49	292 B	Real filetype:html	http://update.gfi.com/license/gfi.key
unauthenticated	127.0.0.1	17:14:49	291 B	Real filetype:html	http://update.gfi.com/license/gfi.key

Screenshot 14 - Monitoring: Past Connections view

Navigate to **Monitoring ► Past Connections** to access the **Past Connections** view.

The information displayed includes:

COLUMN	DESCRIPTION
User	The user being monitored and whose request was processed
IP	The IP being monitored and whose request was processed
Time	The time the request was processed
Size	The total size of request that was processed
Status	The final status of the connection (for example, the file type, the error code, redirection or not modified) that was processed
URL	The URL of the request that is currently being processed

Table Sorting

The list is sorted by **Time** in descending order.

3.4 Hidden Downloads

The **Hidden Downloads** report enables you to monitor all unattended downloads from user machines. An unattended download can be one of the following:

- › Valid updates started automatically from the user's machine
- › Unwanted downloads by hidden applications
- › Interrupted / forgotten downloads initialized by the user. These are downloads that are started by the user and not saved within 15 minutes
- › Malicious downloads that will take advantage of computer software vulnerabilities using sequences of commands.

Hidden Downloads

This page shows downloads which were unattended by user and might show potential hidden unwanted applications or exploits running on client's computers. Unattended means downloads which [produced download status window](#) where user didn't click on save to disk button within 15 minutes after download. Such downloads are also from valid applications (automatic updates etc...). For those, if trusted, it's advised to move their download URL domain locations to the [white list](#).

Group By: URL User Agent IP **View data for:** Today

Display: All Only Executables and Packages

Last Time	Count	Real Filetype	Content Type	URL
▶ 2010-10-14 15:38:08	1	Pdf document	application/pdf	http://www.gfi.com/documents/smartguides/webmon_smartguide_en.pdf
▲ 2010-10-14 15:37:55	1	Pdf document	application/pdf	http://www.gfi.com/webmon/webmonrmanual.pdf
Time	User	IP	Size	User Agent
2010-10-14 15:37:55	tcdomaina.com/administrator	192.168.200.7	1.68 MB	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727)
▶ 2010-10-14 15:37:54	1	Pdf document	application/pdf	http://www.gfi.com/webmon/webmonmanual.pdf
▶ 2010-10-14 15:37:51	1	Pdf document	application/pdf	http://www.gfi.com/webmon/webmongsg.pdf

Screenshot 15 - Monitoring: Hidden Downloads view

Navigate to **Monitoring ► Hidden Downloads** to access the **Hidden Downloads** view.

The information displayed includes:

COLUMN	DESCRIPTION
Last Time	If the URL radio button is selected, the last time when the same URL was accessed is displayed. However, if the User Agent radio button is selected then the last time when the same user agent was used is displayed
Count	The number of times the hidden download was accessed
Real Filetype	The file type of a hidden download
Content Type	The content type of the hidden download as suggested from the web content-type. For more information, refer to the Adding New Content-types section in the WebSecurity Edition - File scanning and download control chapter
URL	The URL of the downloaded file

Expand an entry to view the details for the number of times the hidden download was accessed. The information displayed includes:

COLUMN	DESCRIPTION
Time	The date and time the Hidden download was accessed
User	The user that is being monitored and on whose machine the hidden download was launched
IP	The IP that is being monitored and on whose machine the hidden download was launched
Size	The size of the downloaded file
User Agent	The application/agent that launched the hidden download

From the **Group By** radio buttons select one of the following display options:

OPTION	DESCRIPTION
URL	Displays the URL of the downloaded file
User Agent	Displays the agent that started the hidden download
IP	Displays the IP address of the URL that started the hidden download

From the **Display** radio buttons select one of the following options:

OPTION	DESCRIPTION
All	Displays entries for all file types
Only Executables and Packages	Displays entries for executables and packages only

Further Information

Select the **URL** hyperlink to view the **Permanent Whitelist** dialog. For more information, refer to the [Add Hidden Downloads to Whitelist](#) section in this chapter












3.4.1 Add Hidden Downloads to Whitelist

Whitelist Save Settings Cancel

Use this page to specify the user, IP, or site that you want to exclude from all the policies configured in GFI WebMonitor. Use this feature carefully, since what is included in the list below will bypass all GFI WebMonitor security checks.

Permanent Whitelist Temporary Whitelist

Site ▼ Add

 *.adobe.com	
 *.gfi.com	
 *.macromedia.com	
 *.microsoft.com	
 *.sun.com	
 *.windowsupdate.com	

Screenshot 16 - Whitelist hidden downloads dialog

Click the **URL** of a hidden download to launch the **Permanent Whitelist** dialog. Then click **Add** to whitelist the selected URL.

3.5 Search

The **Search** node enables you to search the user browsing history. This reporting tool is used to determine web browsing patterns, such as which domains or categories are being browsed.

Search



Use this page to search through browsing history by User/IP and Category or Site and by date.

Search For:
 Users Sites and Domains Categories

Where:
Site Contains:

NOTE: Substrings are supported, for example 'domain.com' will return www.domain.com, mail.domain.com, news.domain.com, etc.

Category = All Categories

From:  **To:** 

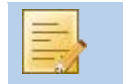
Search

Screenshot 17 - Monitoring: Search view

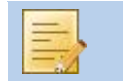
To perform a search:

Navigate to **Monitoring ► Search** and from the **Search For** options, select:

OPTION	DESCRIPTION
Users	Specify a domain name in the Where Site = field. Optionally, select a Category from the drop down list and specify a date range
Sites and Domains	Specify the User/IP from a drop-down list or key in the IP address in the Where User/IP = field. Optionally, select a Category from the drop down list and specify a date range
Categories	Specify the User/IP from a drop-down list or key in the IP address in the Where User/IP = field. Optionally, enter the domain name of a particular website in the Site = field and enter a date range



For **User**, enter the username in the domain\user format.



IP ranges are not supported.

4. Click **Search**.

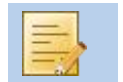
Information is displayed in different views, depending on search criteria:

VIEW	DESCRIPTION
Users	Returns a list of Users or IP numbers. Result pane shows also the total surf time, the data downloaded and uploaded in KB, the number of hits and the number of sites accessed
Sites	Returns a list of sites accessed. Result pane shows also the total surf time, the data downloaded and uploaded in KB, the number of hits and the number of users who accessed each site
Category	Returns a list of categories accessed. Result pane shows also the total surf time, the data downloaded and uploaded in KB, the number of hits for each category, the number of users and the number of sites accessed

5. Search results can be exported as a CSV file. Click **Export to CSV** to create a file and save it in a desired location.

3.6 Access Monitoring

The **Access Monitoring** node grants you access to a set of reports that enable you to monitor internet activity.



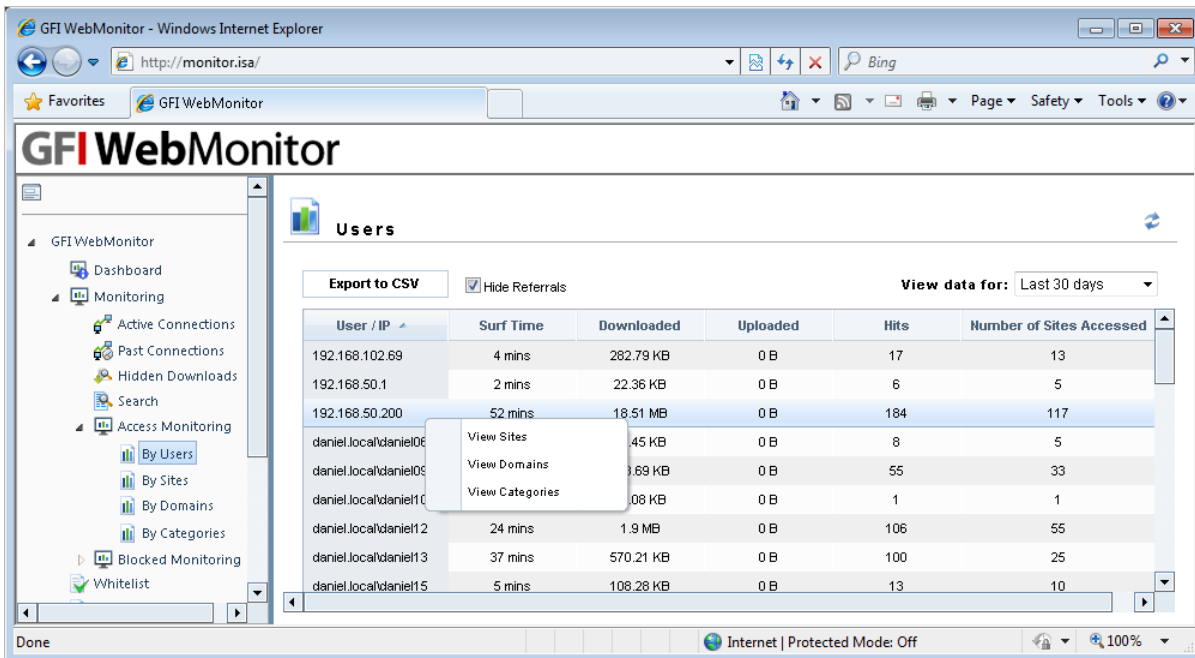
If Anonymization is enabled, personal data (such as User Names and IPs) will be masked. For more information refer to the [Anonymization](#) section in this manual.

3.6.1 Access Monitoring By Users

The report returns a list of Users or IP numbers. Result also shows the total surf time, the data downloaded and uploaded in KB, the number of hits and the number of sites accessed.

1. Navigate to **Monitoring ► Access Monitoring ► By Users**
2. Further drill down can be achieved by hovering the mouse pointer over a particular row. Click **View Sites**, **View Domains** or **View Categories**.

The results can be filtered by date and sorted by any one of the column headings. For example, sorting by **Surf Time** would indicate which user spent most time surfing. You can then drill down on a particular user and check the sites they accessed.



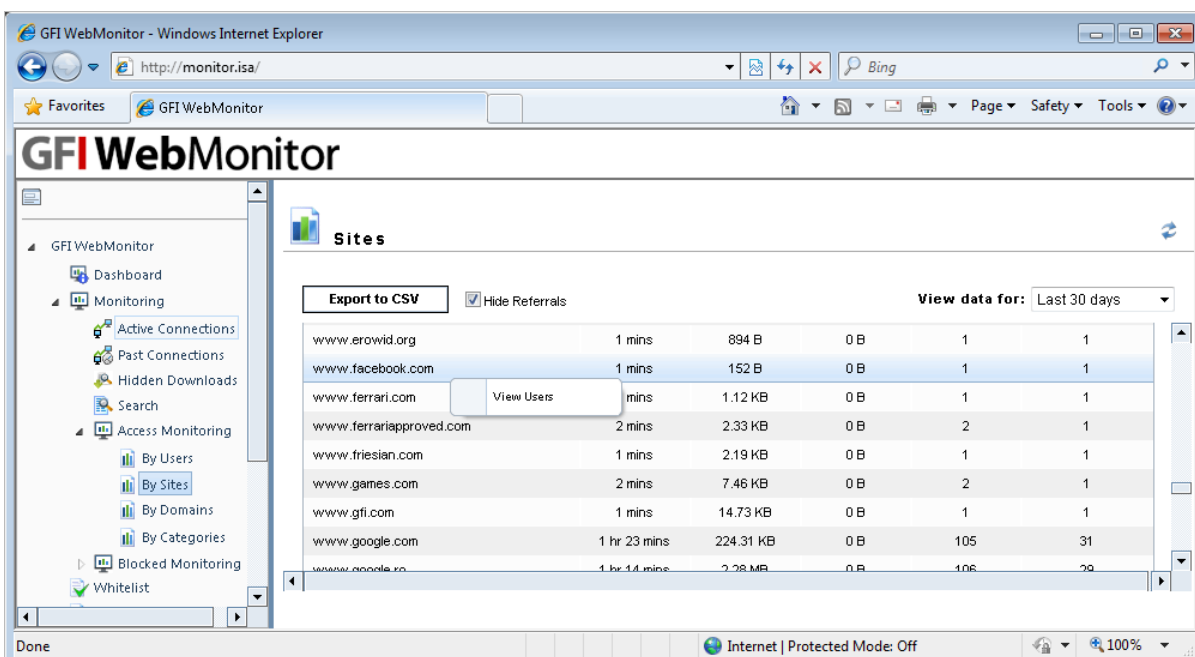
Screenshot 18 - Monitoring By Users showing further drilldown options

3.6.2 Access Monitoring By Sites

The report returns a list of sites accessed. Result also shows the total surf time, the data downloaded and uploaded in KB, the number of hits and the number of users who accessed each site.

1. Navigate to **Monitoring ► Access Monitoring ► By Sites**
2. Further drill down can be achieved by hovering the mouse pointer over a particular row. Click **View Users**.

The results can be filtered by date and sorted by any one of the column headings. For example, sorting by **Hits** would indicate the most popular websites.



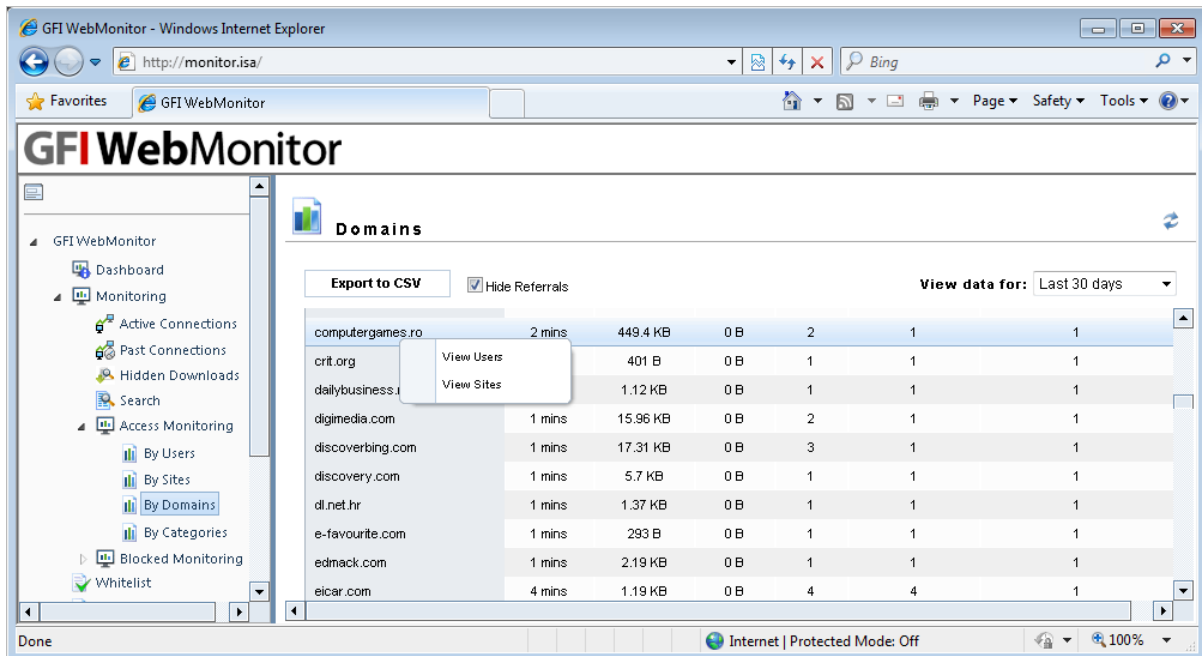
Screenshot 19 - Monitoring By Users showing further drilldown options

3.6.3 Access Monitoring By Domains

The report returns a list of domains accessed. Result also shows the total surf time, the data downloaded and uploaded in KB, the number of hits, the number of users who accessed each domain and the number of sites accessed.

1. Navigate to **Monitoring ► Access Monitoring ► By Domains**
2. Further drill down can be achieved by hovering the mouse pointer over a particular row. Click **View Users** or **View Sites**.

The results can be filtered by date and sorted by any one of the column headings. For example, sorting by **Downloaded** would show from which domains your employees are downloading the most.



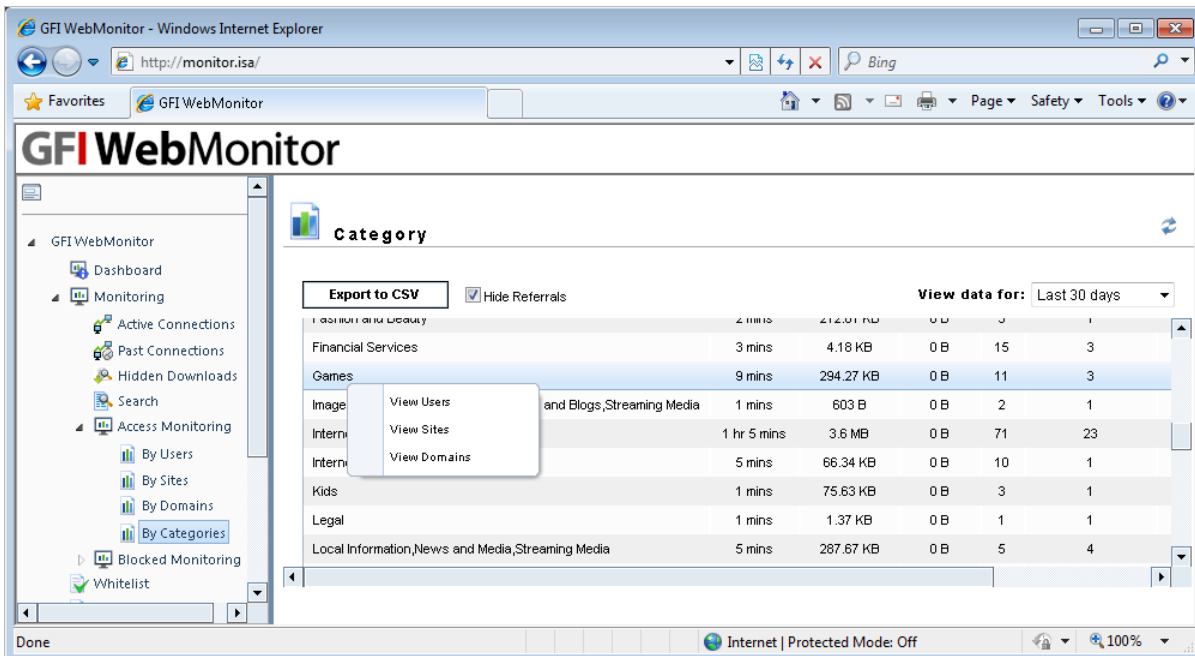
Screenshot 20 - Monitoring By Users showing further drilldown options

3.6.4 Access Monitoring By Categories


The report returns a list of categories accessed. Result also shows the total surf time, the data downloaded and uploaded in KB, the number of hits for each category, the number of users and the number of sites accessed.

1. Navigate to **Monitoring ► Access Monitoring ► By Categories**
2. Further drill down can be achieved by hovering the mouse pointer over a particular row. Click **View Users**, **View Sites** or **View Domains**.

The results can be filtered by date and sorted by any one of the column headings. For example, sorting by **Hits** would show the most popular categories.



Screenshot 21 - Monitoring By Users showing further drilldown options

 Click a row to further drill down on results. Each of these views can then be exported in CSV format.

3.7 Blocked Monitoring

The **Blocked Monitoring** node grants you access to a set of reports that enable you to monitor internet activity. The types of reports available are:

REPORT	DESCRIPTION
Blocked Monitoring by Users	Returns a list of Users or IP numbers. Results also show the total number of Breaches, the number of Policies Breached and the total number of Sites Blocked per User / IP. The results can be filtered by date and sorted by any one of the column headings.
Blocked Monitoring by Policy	Returns a list of Policy Types. Results also show the Policy name, total number of Users Blocked, the number of Breaches and the total number of Sites Blocked per Policy. The results can be filtered by date and sorted by any one of the column headings.
Blocked Monitoring by Policy Type	Returns a list of Policy Types. Results also show the total number of Users Blocked, the number of Breaches, the number of Policies Breached and the total number of Sites Blocked per Policy Type. The results can be filtered by date and sorted by any one of the column headings.
Blocked Monitoring by Category	Returns a list of blocked categories. Results also show the total number of Users Blocked, the number of Breaches and the total number of Sites Blocked per category. The results can be filtered by date and sorted by any one of the column headings.
Blocked Activity Log	Returns a list of entries sorted by User. Results also show the date the user tried to access a blocked site, the name of the policy and the URL name of each entry.

4 Allowing and Blocking Users, IP Addresses and Sites

4.1 Introduction

The **Whitelist** and **Blacklist** nodes enable you to set up content scanning policies that override all policy settings set up in WebFilter and WebSecurity editions.

4.2 Whitelist

The **Whitelist** is a list of sites, users and IP addresses approved by the administrator to be excluded from all policies configured in GFI WebMonitor. Besides the **Permanent Whitelist**, there is also a **Temporary Whitelist** that is used to temporarily approve access to a site for a user or IP address.



In GFI WebMonitor, the Temporary Whitelist takes priority over the Permanent Whitelist. Furthermore, both Whitelists take priority over the Blacklist. Thus, if a site is listed in any of the Whitelists and that same site is listed in the Blacklist, the site will be allowed.

4.2.1 Preconfigured Items

By default, GFI WebMonitor includes a number of preconfigured sites in the Permanent Whitelist. These include GFI websites to allow automatic updates to GFI WebMonitor and Microsoft websites to allow automatic updates to Windows. Removing any of these sites may preclude important updates from being automatically effected.

4.2.2 Adding Items to the Permanent Whitelist

Whitelist Save Settings Cancel

Use this page to specify the user, IP, or site that you want to exclude from all the policies configured in GFI WebMonitor. Use this feature carefully, since what is included in the list below will bypass all GFI WebMonitor security checks.

Permanent Whitelist Temporary Whitelist




Site Add

*.adobe.com	
*.gfi.com	
*.gfisoftware.com	
*.macromedia.com	
*.microsoft.com	
*.sun.com	
*.windowsupdate.com	

Screenshot 22 - Permanent Whitelist view


To add an item to the Permanent Whitelist:

1. Navigate to the **Whitelist** node and select the **Permanent Whitelist** tab.
2. From the drop-down list, select the **User(s)**, **Client IP(s)** and/or **Site(s)** which will be added to the whitelist and click **Add**. Repeat for all the required user(s), IP(s) and/or site(s).
3. Click **Save Settings**.

	When keying in a User , specify the username in the format domain\user.
	When keying in a Client IP , you can use IP ranges (for example, “10.0.0.10-12” includes these IP addresses: “10.0.0.10”, “10.0.0.11” and “10.0.0.12”).
	When keying in a Site , you can use wildcards (for example, “*.website.com”). For more information, refer to the Using Wildcards section in this chapter.

4.2.3 Deleting Items From the Permanent Whitelist

To delete an item from the Permanent Whitelist:

1. Navigate to the **Whitelist** node and select the **Permanent Whitelist** tab.
2. Click the **Delete** icon  next to the item to delete.
3. Click **Save Settings**.

4.2.4 Adding Items to the Temporary Whitelist



The screenshot shows the 'Whitelist' configuration window. At the top, there is a green checkmark icon and the title 'Whitelist'. To the right are 'Save Settings' and 'Cancel' buttons. Below the title is a warning message: 'Use this page to specify the user, IP, or site that you want to exclude from all the policies configured in GFI WebMonitor. Use this feature carefully, since what is included in the list below will bypass all GFI WebMonitor security checks.' There are two tabs: 'Permanent Whitelist' and 'Temporary Whitelist', with the latter selected. Below the tabs is another warning: 'Apart from the sites that you approve manually for a temporary period, this list also includes the sites that were approved from the GFI WebMonitor Quarantine.' An 'Add' button is located below this text. A table with columns 'Grant To', 'Access To', and 'For (hours)' is shown. The first row has 'designer' under 'Grant To', 'www.google.com' under 'Access To', and '10.0' under 'For (hours)', with a trash icon to the right. The second row has '192.168.99.99' under 'Grant To', 'www.gfi.com' under 'Access To', and '250.0' under 'For (hours)', also with a trash icon to the right. At the bottom left is a 'Delete All' button.

Grant To	Access To	For (hours)	
 designer	www.google.com	10.0	
 192.168.99.99	www.gfi.com	250.0	




Screenshot 23 - Temporary Whitelist view

To add an item to the Temporary Whitelist:

1. Navigate to the **Whitelist** node and select the **Temporary Whitelist** tab.
2. Click **Add**.



Screenshot 24 - Temporary Whitelist: Granting Temporary Access dialog

3. Select a User or an IP from the **Grant to:** drop-down list. Provide the user or IP to be granted temporary access as well as the URL of the site and the number of hours.

-  When keying in a **User**, specify the username in the format domain\user.
-  When keying in an **IP**, you can use IP ranges (for example, “10.0.0.10-12” includes these IP addresses: “10.0.0.10”, “10.0.0.11” and “10.0.0.12”).
-  When keying in a **Site**, you can use wildcards (for example, “*.website.com”). For more information, refer to the [Using Wildcards](#) section.


4. Click **Add** to add the new item to the list.

5. Click **Save Settings**.

-  The number of hours during which the user or IP has access to a site become applicable from the moment **Save Settings** is clicked.
-  The **For (hours)** column in the **Whitelist** view displays the Time remaining before access is revoked.


4.2.5 Deleting Items From the Temporary Whitelist

To delete an item from the Temporary Whitelist:

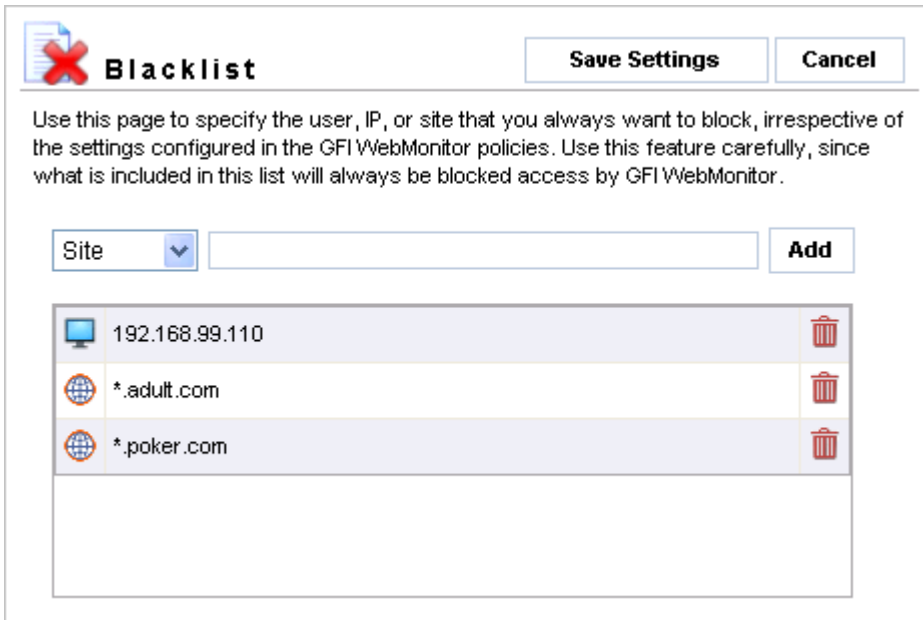
1. Navigate to the **Whitelist** node and select the **Temporary Whitelist** tab.
2. Click the **Delete** icon  next to the item to delete.
3. Click **Save Settings**.

4.3 Blacklist

The **Blacklist** is a list of sites, users and IP addresses that should always be blocked irrespective of the WebFilter and WebSecurity policies configured in GFI WebMonitor.

-  In GFI WebMonitor, the Blacklist takes priority over all WebFilter and WebSecurity policies.




4.3.1 Adding Items to the Blacklist



Screenshot 25 - Blacklist view

To add an item to the Blacklist:


1. Navigate to the **Blacklist** node.
2. From the drop-down list, select the **User(s)**, **Client IP(s)** and/or **Site(s)** which will be added to the blacklist and click **Add**. Repeat for all the required user(s), IP(s) and/or site(s).

	When keying in a User , specify the username in the format domain\user.
	When keying in a Client IP , you can use IP ranges (for example, “10.0.0.10-12” includes these IP addresses: “10.0.0.10”, “10.0.0.11” and “10.0.0.12”).
	When keying in a Site , you can use wildcards (for example, “*.website.com”). For more information, refer to the Using Wildcards section in this chapter.

3. Click **Save Settings**.

4.3.2 Deleting Items From the Blacklist

To delete an item from the Blacklist:

1. Navigate to the **Blacklist** node.
2. Click the **Delete** icon  next to the item to delete.
3. Click **Save Settings**.

4.4 Using Wildcards

When keying in a site to the whitelist or blacklist, you can use the wildcard character [*] as shown in the examples below:

EXAMPLE	DESCRIPTION
*.com	Allow/block all ‘.com’ top-level domains
*.website.com	Allow/block all sub domains of the ‘website.com’ domain

5 WebFilter Edition - Site Rating and Content Filtering

5.1 Introduction

The **WebFilter Edition** node and its sub-nodes enable you to manage the internet access of users, groups or IP addresses on your network via control policies. The control policies include:

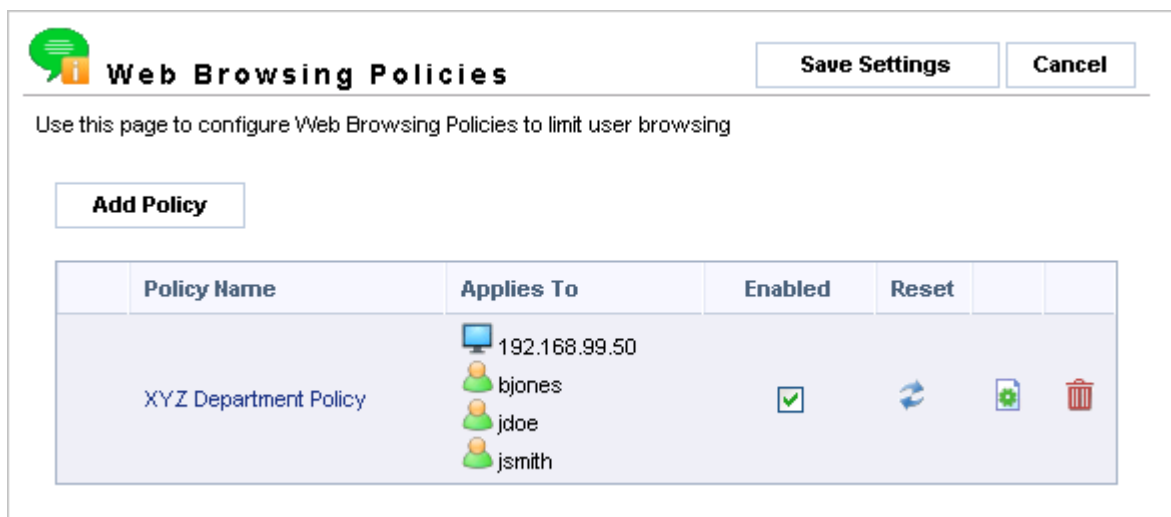
- » **Web Browsing Policies:** to control browsing time and download bandwidth thresholds
- » **Web Filtering Policies:** to control internet access during specific periods.








5.2 Web Browsing Policies

The **Web Browsing Policies** node enables you to create policies per user(s), group(s) and/or IP address(es) to:

- » restrict browsing time
- » restrict download thresholds

These restrictions are based on specific sites and/or web categories. If the policy is exceeded, GFI WebMonitor then issues a notification and blocks access to sites or categories. Furthermore, specific sites can be excluded per policy.



Policy Name	Applies To	Enabled	Reset		
XYZ Department Policy	 192.168.99.50  bjones  jdoe  jsmith	<input checked="" type="checkbox"/>			

Screenshot 26 - Web Browsing Policies view



More than one Web Browsing Policy can be applied to a user, a group and/or IP address.

In cases where more than one Web Browsing Policy is applied to the same user, group or IP, the top most policy takes priority over subsequent policies. For example:

EXAMPLE POLICIES	GFI WEBMONITOR ACTIONS
<p>Example 1</p> <p>Policy 1 (highest priority)</p> <ul style="list-style-type: none"> » Applies to: User A » Allows browsing of 'Sports' websites for 15 minutes per day <p>Policy 2 (lowest priority)</p> <ul style="list-style-type: none"> » Applies to: User A » Allows browsing of 'Sports' websites for 10 minutes per day 	<p>Scenario 1</p> <p>Policy 1 and Policy 2 are enabled and User A browses a 'Sports' website for 1 minute:</p> <ul style="list-style-type: none"> » User A is allowed to browse 'Sports' websites for a further 14 minutes <p>Scenario 2</p> <p>Policy 1 and Policy 2 are enabled and User A browses a 'Sports' website for 11 minutes. Next, Policy 1 is disabled:</p> <ul style="list-style-type: none"> » Policy 2 comes into effect at once » User A is no longer allowed to browse 'Sports' websites.
<p>Example 2</p> <p>Policy 1 (highest priority)</p> <ul style="list-style-type: none"> » Applies to: User A » Allows browsing of 'News and Media' websites for 5 minutes per day <p>Policy 2 (lowest priority)</p> <ul style="list-style-type: none"> » Applies to: User A » Allows browsing of 'Sports' websites for 20 minutes per day 	<p>Scenario</p> <p>Policy 1 and Policy 2 are enabled and User A browses a 'Sports' website for 1 minute:</p> <ul style="list-style-type: none"> » Policy 1 counter is not increased » Policy 2 counter is increased by 1 minute » User A is allowed to browse 'News and Media' websites for 5 minutes » User A is allowed to browse 'Sports' websites for a further 19 minutes

5.2.1 Adding a Web Browsing Policy

Screenshot 27 - Web Browsing Policies: General tab

To add a Web Browsing Policy:

1. Navigate to **WebFilter Edition ► Web Browsing Policies**.
2. Click **Add Policy**.

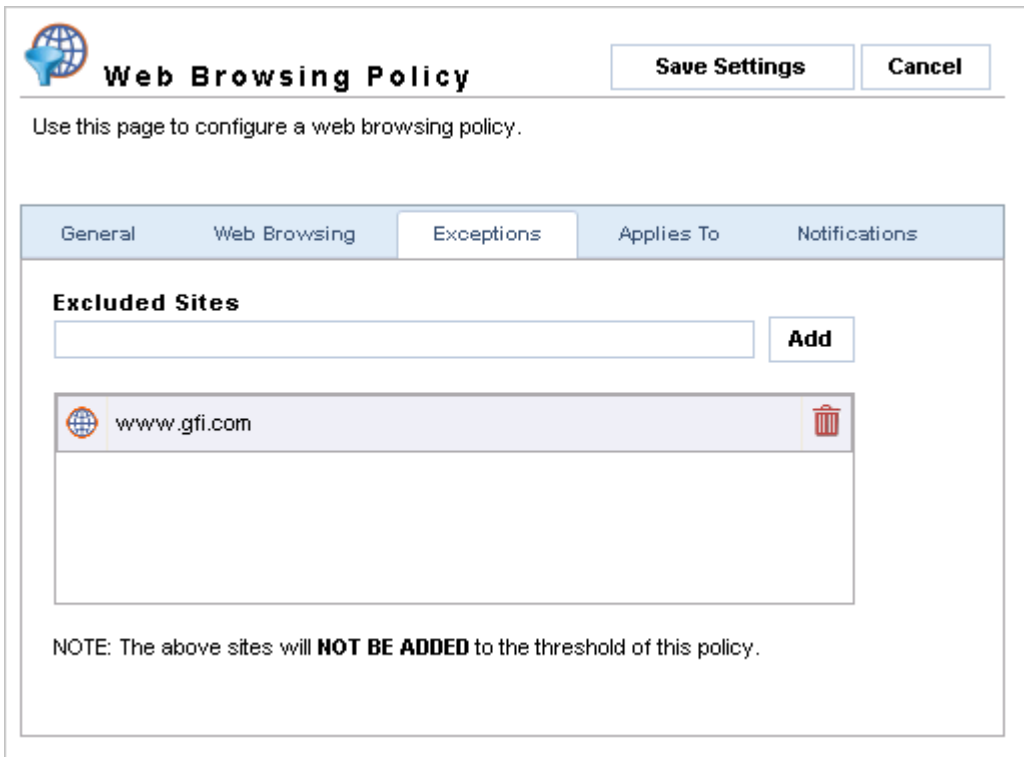
3. In the **General** tab provide a **Policy Name** and a **Policy Description**

Screenshot 28 - Web Browsing Policies: Web Browsing tab

4. Select the **Web Browsing** tab and from the **Threshold** area, specify the browsing or downloading limits. The available options are:

OPTION	DESCRIPTION
Allow browsing of sites/categories	Specify the allowed amount of minutes/hours per day/week/month
Allow downloading from sites/categories	Specify the allowed amount of KB/MB per day/week/month

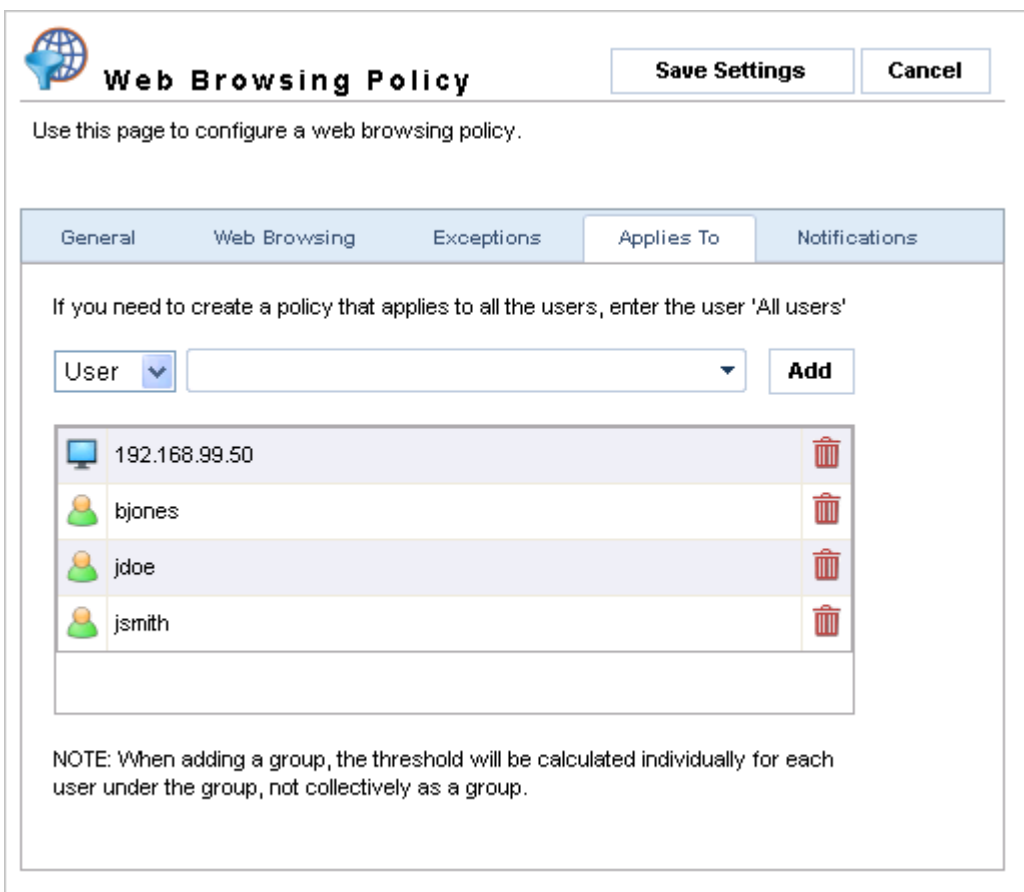
5. In the **Categories/Sites to be limited** area, specify the **Site(s)** and/or **Category(ies)** that will be restricted by the new policy and click **Add**. Repeat for all the required site(s) and/or category(ies).



Screenshot 29 - Web Browsing Policies: Exceptions tab



6. Select the **Exceptions** tab.

7. In the **Excluded Sites** field specify any URLs, which are to be excluded from this policy. This enables users to access sites without reducing from the total browsing time and download bandwidth allowed, thus overriding other restrictions.



Screenshot 30 - Web Browsing Policies: Applies To tab

8. Select the **Applies To** tab and specify the **User(s)**, **Group(s)** and/or **IP(s)** for whom the new policy applies and click **Add**. Repeat for all the required user(s), group(s) and/or IP(s).

-  When keying in a **User**, specify the username in the format domain\user.
-  When keying in an **IP**, you can use IP ranges (for example, “10.0.0.10-12” includes these IP addresses: “10.0.0.10”, “10.0.0.11” and “10.0.0.12”).

Screenshot 31 - Web Browsing Policies: Notifications tab


9. (Optional) Select the **Notifications** tab and define the notifications to send when a user infringes this policy. The available options are:

OPTION	DESCRIPTION
Notify the following administrators when a user infringes this policy	Select this option to send a notification to administrators. Add the administrator’s email address and provide the body text of the notification email
Notify the user accessing the site if they exceed the threshold set by this policy	Select this option to send a notification to the user infringing this policy and provide the body text of the notification email

10. Click **Save Settings**. The new policy will now be listed in the main **Web Browsing Policies** view.

5.2.2 Editing a Web Browsing Policy

To edit a Web Browsing Policy:

1. Navigate to **WebFilter Edition ► Web Browsing Policies**.
2. Click the **Edit** icon  next to the policy to edit.
3. Click **Save Settings**.

5.2.3 Enabling/Disabling a Web Browsing Policy

To enable or disable a Web Browsing Policy:

1. Navigate to **WebFilter Edition ► Web Browsing Policies**.
2. Check or uncheck the checkbox from the **Enabled** column for the policy to enable or disable.
3. Click **Save Settings**.

5.2.4 Deleting a Web Browsing Policy

To delete a Web Browsing Policy:

1. Navigate to **WebFilter Edition ► Web Browsing Policies**.
2. Click the **Delete** icon  next to the policy to delete.
3. Click **Save Settings**.

5.2.5 Resetting a Web Browsing Policy


By resetting a Web Browsing Policy, all the threshold counters within the policy are reset. This is applied for all users and IP addresses specified within the policy.

For example, a Web Browsing Policy that is applied to three particular users is configured to allow browsing of 'Sports' websites for 10 minutes per day. All three users have already browsed Sports websites for a number of minutes, but when this policy is reset, the 10 minutes counter is reset to zero. All three users will now be allowed to browse 'Sports' websites for a further 10 minutes.



For information on how to reset the used threshold for a single user/IP specified within a Web Browsing Policy, refer to the [Web Browsing Thresholds](#) section in this chapter.

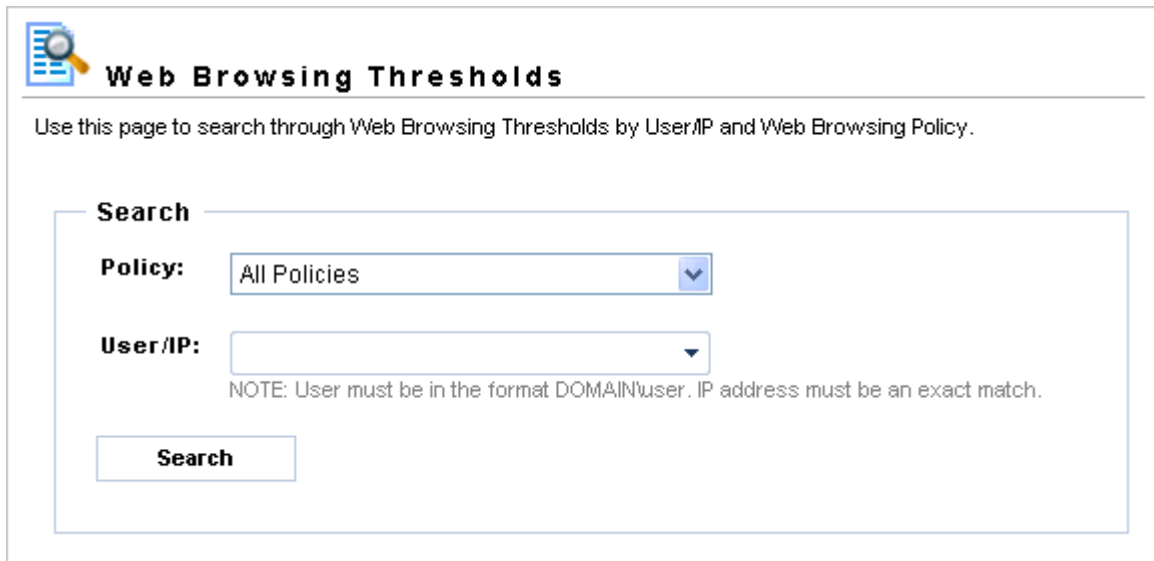
To reset a Web Browsing Policy:

1. Navigate to **WebFilter Edition ► Web Browsing Policies**.
2. Click the **Reset** icon  next to the policy to reset and **OK** to confirm.

5.3 Web Browsing Thresholds

The **Web Browsing Thresholds** node enables you to:

- > search for and display counters for a user or IP within Web Browsing Policies
- > reset used browsing time or download bandwidth threshold for a single user or IP.



Screenshot 32 - Monitoring: Search view

5.3.1 Searching for Web Browsing Policies and/or Users/IPs

To search an item:

1. Navigate to **WebFilter Edition ► Web Browsing Policies ► Web Browsing Thresholds**.
2. From the **Policy** drop-down list select the Web Browsing Policy required.
3. From the **User/IP** drop-down list, key in or select the User or IP address.
4. Click **Search** to display the **Search Results** area.

The information displayed within the **Search Results** area includes:

COLUMN	DESCRIPTION
User/IP	The user/IP being monitored
Policy	The Web Browsing Policy where the user/IP is specified
Threshold	The amount of browsing time and/or download bandwidth threshold specified in the Web Browsing Policy
Threshold Used	The total browsing time or total download bandwidth used by the user/IP at the time of the search



When keying in a **User**, specify the username in the format domain\user.



IP ranges are not supported.

5.3.2 Resetting Web Browsing Policy Threshold for a Single User/IP

By resetting a Web Browsing Threshold for a single user and/or IP, all the threshold counters within the policy for that user are reset.

For example, a Web Browsing Policy is applied to three users and is configured to allow browsing of 'Sports' websites for 10 minutes per day. It is reset for one user, and the counter is reset to zero for that user only. This means that particular user will be allowed to browse 'Sports' websites for a further 10 minutes, whilst the other two users will no longer be allowed to browse 'Sports' websites



For more information on how to reset the used threshold for ALL user(s) and/or IP(s) specified within a Web Browsing Policy, refer to the [Resetting a Web Browsing Policy](#) section in this chapter.

To reset the Web Browsing Policy threshold for a single user or IP:

1. Search for the relevant Web Browsing Policy and/or user/IP. For more information, refer to the [Searching for Web Browsing Policies and/or Users/IPs](#) section in this chapter.
2. From the **Search Results** area, locate the relevant **User/IP** and **Policy** combination.
3. Click **Reset** next to the user/IP and policy combination to reset.

5.4 Web Filtering Policies

The **Web Filtering Policies** node enables you to create policies per user(s), group(s) and/or IP(s) to manage Internet access during specific periods, based on web categories. If an accessed site triggers a policy, GFI WebMonitor then uses the configured Web Filtering policy to determine what action to take. This may be one of the following actions:

- » Allow access to sites within specified categories per user(s), group(s) and/or IP(s)
- » Block access to sites within specified categories per user(s), group(s) and/or IP(s)
- » Quarantine access to sites within specified categories per user(s), group(s) and/or IP(s); that is, upon the discretion of the administrator temporary access is allowed to blocked sites
- » Exclude or include specific sites per policy.

Policy Name	Applies To	Enabled		
XYZ Department Policy	192.168.99.50 bjones jdoe jsmith	<input checked="" type="checkbox"/>		
Default Web Filtering Policy	Applies to everyone	<input checked="" type="checkbox"/>		

Screenshot 33 - Web Filtering Policies view



It is recommended that only one Web Filtering Policy is applied to a user, a group and/or IP address. In cases where more than one Web Filtering Policy is applied to the same user, group or IP, the top most policy takes priority over subsequent policies.

5.4.1 Adding a Web Filtering Policy

To add a Web Filtering Policy:

1. Navigate to **WebFilter Edition ► Web Filtering Policies**.
2. Click **Add Policy**.

Web Filtering Policy Save Settings Cancel

Use this page to configure a web filtering policy.

General | Web Filtering | Exceptions | Applies To | Notifications

Policy Name
XYZ Department Policy

Policy Description
Web Filtering policy applicable for the XYZ Department


Policy Schedule

■ Policy Active □ Policy Inactive

	0	2	4	6	8	10	12	14	16	18	20	22	0
Sunday	v	v	v	v	v	v	v	v	v	v	v	v	v
Monday	v												
Tuesday	v												
Wednesday	v												
Thursday	v												
Friday	v												
Saturday	v												

Screenshot 34 - Web Filtering Policies: General tab

3. In the **General** tab provide a **Policy Name** and a **Policy Description**.
4. In the **Policy Schedule** area, specify the time period during which the new policy will be enforced.

 **Web Filtering Policy**

Use this page to configure a web filtering policy.

General | **Web Filtering** | Exceptions | Applies To | Notifications

A site can have multiple categories associated with it, for example, news and sports. If one or more of the categories associated with a site is listed in the blocked categories list below, the site will be blocked.

<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Category
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Abortion
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Abused Drugs
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Adult and Pornography
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Alcohol and Tobacco
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Auctions
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Bot Nets
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Business and Economy
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	CDNs
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Computer and Internet Info
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Computer and Internet Security
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Confirmed SPAM Sources

Legend

- Allow
- Quarantine
- Block


Screenshot 35 - Web Filtering Policies: Web Filtering tab

5. Select the **Web Filtering** tab and set the action to take for each category as required:

- > Allow
- > Quarantine
- > Block

6. (Optional) Click the **Show Advanced Options** button to configure actions for combined categories per policy. For more information, refer to the [Configuring Advanced Web Filtering Policy Conditions](#) section in this chapter.



The **Override Rules** area enables you to fine-tune combined actions and categories per policy. These advanced **Web Filtering Policy** conditions give you greater flexibility in defining which sites should be allowed or blocked.

 **Web Filtering Policy**

Use this page to configure a web filtering policy.





General Web Filtering **Exceptions** Applies To Notifications

Excluded Sites

	www.gfi.com	
---	-------------	---

NOTE: The above sites will **NOT BE BLOCKED** by this policy when their category is blocked in the Web Filtering tab.

Included Sites

	www.hi5.com	
	www.facebook.com	

NOTE: The above sites will be **BLOCKED** by this policy, even when their category is not blocked in the Web Filtering tab.

Screenshot 36 - Web Filtering Policies: Exceptions tab

7. Select the **Exceptions** tab and in the **Excluded Sites** and **Included Sites** fields specify any URLs, which are to be:

- > Excluded (that is, allowed) from the policy. This enables users to access sites overriding other restrictions.
- > Included (that is, blocked) in the new policy. The URLs specified in the included sites will be blocked regardless of the scope of the new policy.



The **Exceptions** tab is similar to a whitelist/blacklist feature that overrides any rules within the policy.

Web Filtering Policy Save Settings Cancel

Use this page to configure a web filtering policy.

General Web Filtering Exceptions **Applies To** Notifications

If you need to create a policy that applies to all the users, you need to edit the settings in the Default Web Filtering Policy.

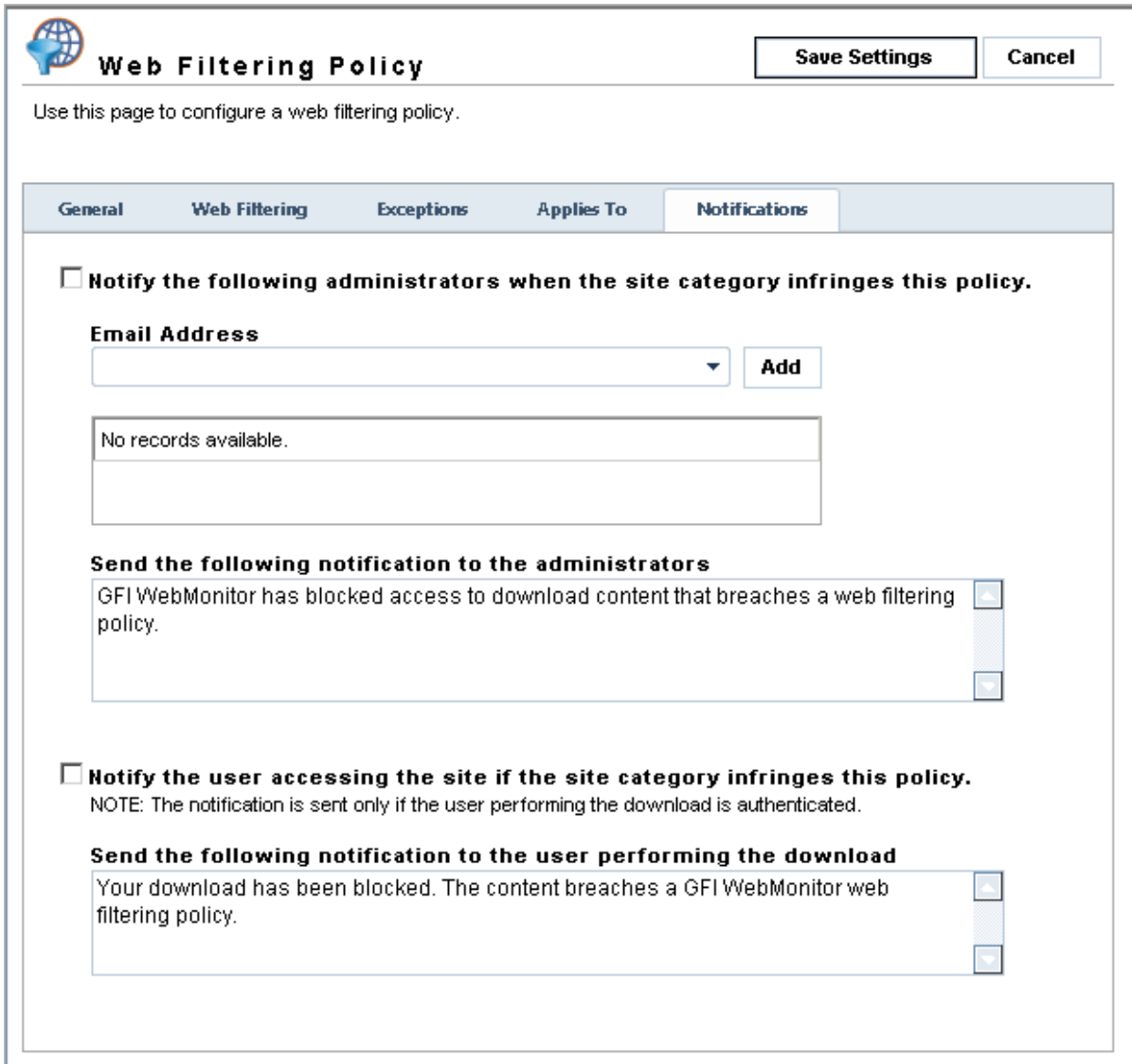
User

	192.168.99.50	
	bjones	
	jdoe	
	jsmith	

Screenshot 37 - Web Filtering Policies: Applies To tab

8. Select the **Applies To** tab and specify the **User(s)**, **Group(s)** and/or **IP(s)** for whom the new policy applies and click **Add**. Repeat for all the required user(s), group(s) and/or IP(s).

	When keying in a User , specify the username in the format domain\user.
	When keying in an IP , you can use IP ranges (for example, "10.0.0.10-12" includes these IP addresses: "10.0.0.10", "10.0.0.11" and "10.0.0.12").



Screenshot 38 - Web Filtering Policies: Notifications tab


9. (Optional) Select the **Notifications** tab and define the notifications to send when a user infringes this policy. The available options are: WebFilter-WebFilteringPolicies-Notifications tab.png

OPTION	DESCRIPTION
Notify the following administrators when the site category infringes this policy	Select this option to send a notification to administrators. Add the administrator's email address and provide the body text of the notification email
Notify the user accessing the site if the site category infringes this policy	Select this option to send a notification to the user infringing this policy and provide the body text of the notification email

10. Click **Save Settings**. The new policy will now be listed in the main **Web Filtering Policies** view.

5.4.2 Editing a Web Filtering Policy

To edit a Web Filtering Policy:

1. Navigate to **WebFilter Edition ► Web Filtering Policies**.
2. Click the **Edit** icon  next to the policy to edit.
3. Click **Save Settings**.


5.4.3 Enabling/Disabling a Web Filtering Policy

To enable or disable a Web Filtering Policy:

1. Navigate to **WebFilter Edition ► Web Filtering Policies**.
2. Check or uncheck the checkbox from the **Enabled** column for the policy to enable or disable.
3. Click **Save Settings**.

5.4.4 Deleting a Web Filtering Policy

To delete a Web Filtering Policy:

1. Navigate to **WebFilter Edition ► Web Filtering Policies**.
2. Click the **Delete** icon  next to the policy to delete.
3. Click **Save Settings**.

5.4.5 Default Web Filtering Policy

GFI WebMonitor - WebFilter Edition ships with a default web filtering policy, which is configured to apply to all users. The policy name is listed as **Default Web Filtering Policy**.

This policy can be edited but it cannot be disabled or deleted. Refer to the [Editing a Web Filtering Policy](#) section in this chapter for information related to editing web filtering policies.



All added Web Filtering Policies take priority over the Default Web Filtering Policy.



Certain fields in the default policy cannot be edited. These include **Policy Name**, **Policy Description** and fields in the **Applies To** tab.

5.5 Configuring Advanced Web Filtering Policy Conditions

The **Override Rules** area enables you to configure rules based on a combination of website categories. This is particularly useful for sites associated with more than one category. These advanced **Web Filtering Policy** conditions give you greater flexibility in defining which categories of sites should be allowed or blocked.



For a site to be blocked by an advanced condition, it must be listed under **ALL** categories defined in the condition.

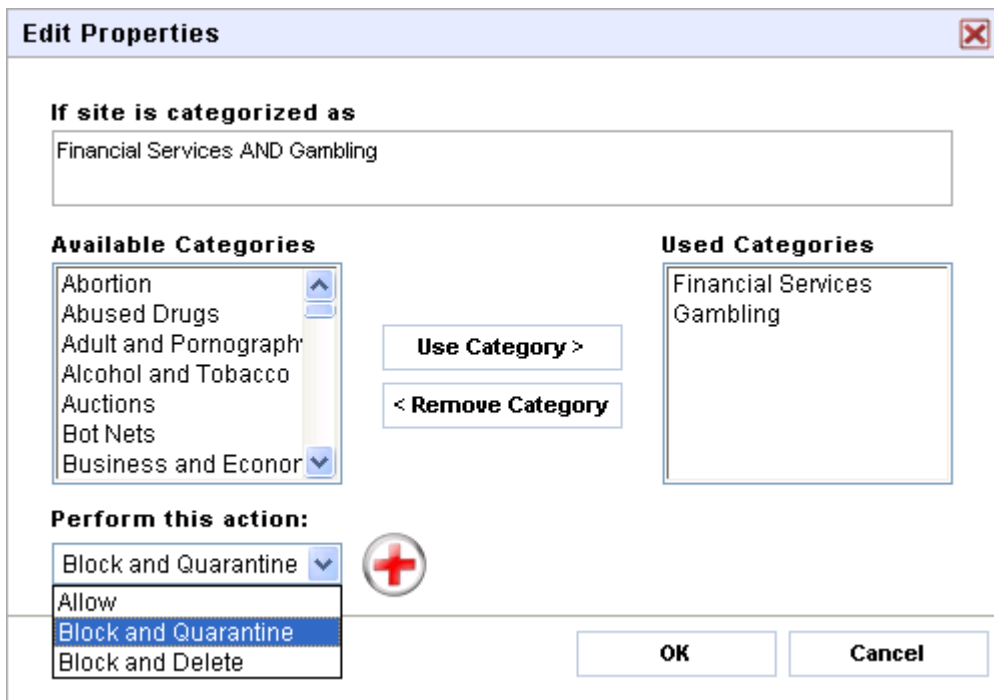


Advanced Web Filtering Policy Rules override the conditions set within the **Categories** list.

5.5.1 Adding an Advanced Web Filtering Policy Condition

To add an advanced Web Filtering Policy condition:

1. Select the **Web Filtering** tab and click **Show Advanced Options** to view the **Override Rules** for that specific policy.
2. Click the **Add Condition** button to view the **Edit Properties** dialog.



Screenshot 39 - Adding an advanced Web Filtering Policy condition

3. Specify a combination of site categories that you would like to allow, block and quarantine or block and delete.

For example, to block and quarantine sites which fall under the categories 'Financial Services' AND 'Gambling':

- a. Select **Financial Services** from **Available Categories** list box and click **Use Category >**
- b. Select **Gambling** from **Available Categories** list box and click **Use Category >**
- c. Select **Block and Quarantine** from the **Perform this action:** drop-down list and click **OK** to apply the condition.

In this example, a site is only blocked if it falls under both categories. Thus, it is NOT blocked if it is categorized as 'Financial Services' only and likewise it is NOT blocked if it is categorized as 'Gambling' only.

4. Click **Save Settings**.


5.5.2 Editing an Advanced Web Filtering Policy Condition

To edit an advanced Web Filtering Policy condition:

1. Select the **Web Filtering** tab and click **Show Advanced Options**.
2. Click the advanced policy to be edited, to view the **Edit Properties** dialog.
3. Edit the advanced condition by doing any of the following:
 - a. Add more or Remove categories
 - b. Change the action from the **Perform this action:** drop-down list.
4. Click **OK** to apply the changes you made.
5. Click **Save Settings**.

5.5.3 Deleting an Advanced Web Filtering Policy Condition

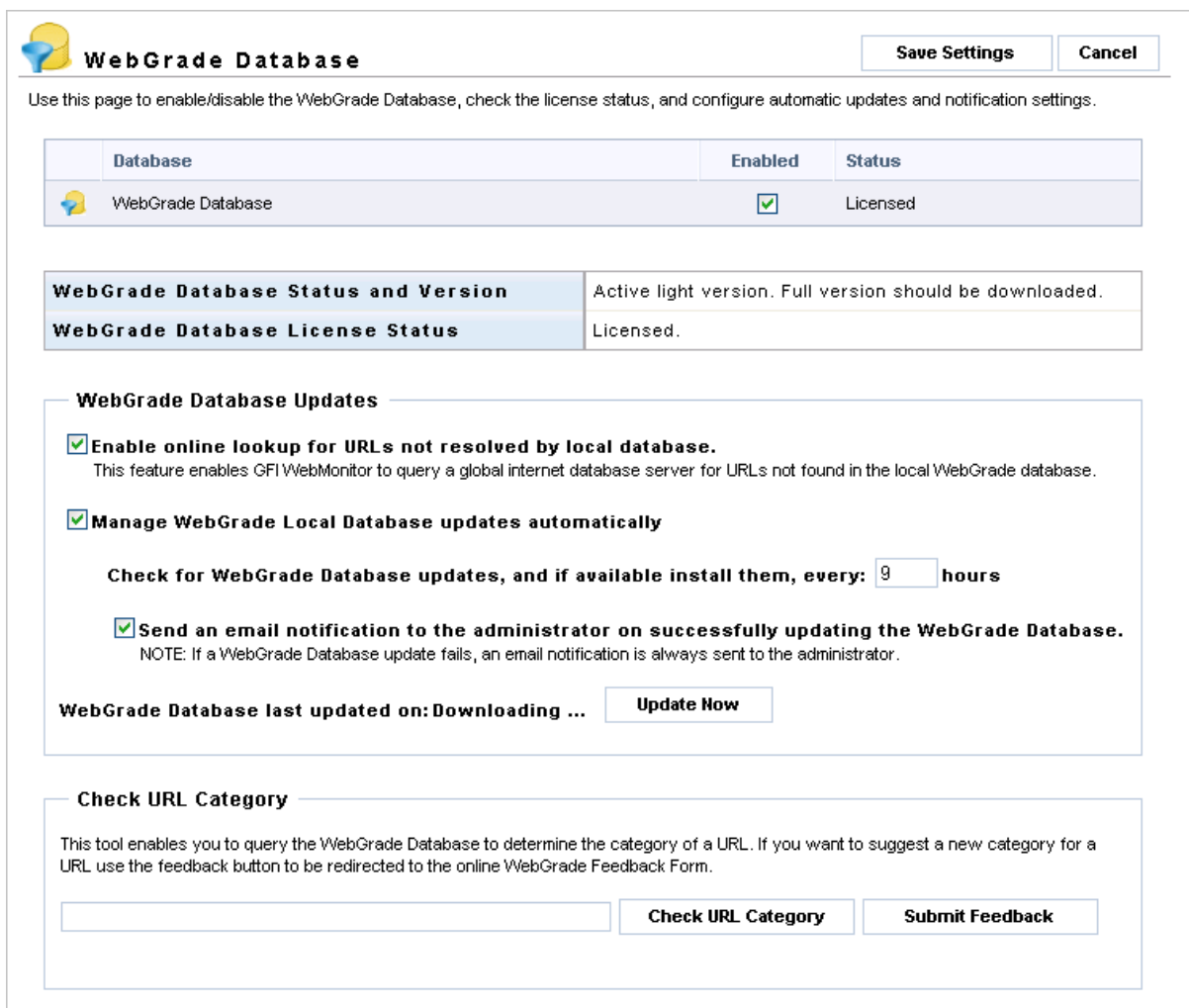
To delete an advanced Web Filtering Policy condition:

1. Select the **Web Filtering** tab and click **Show Advanced Options**.
2. Click the **Delete** icon  next to the advanced policy to delete.
3. Click **Save Settings**.

5.6 WebGrade Database


The **WebGrade Database** node enables you to:

- » Enable/disable the database
- » View the database status, version and license details
- » Enable/disable online lookups for URLs
- » Configure database updates
- » Check the presence or validity of any URL within the active local WebGrade database and send feedback.



WebGrade Database Save Settings Cancel

Use this page to enable/disable the WebGrade Database, check the license status, and configure automatic updates and notification settings.

Database	Enabled	Status
 WebGrade Database	<input checked="" type="checkbox"/>	Licensed

WebGrade Database Status and Version Active light version. Full version should be downloaded.

WebGrade Database License Status Licensed.

WebGrade Database Updates

- Enable online lookup for URLs not resolved by local database.**
This feature enables GFI WebMonitor to query a global internet database server for URLs not found in the local WebGrade database.
- Manage WebGrade Local Database updates automatically**
Check for WebGrade Database updates, and if available install them, every: **hours**
- Send an email notification to the administrator on successfully updating the WebGrade Database.**
NOTE: If a WebGrade Database update fails, an email notification is always sent to the administrator.

WebGrade Database last updated on: Downloading ... Update Now

Check URL Category

This tool enables you to query the WebGrade Database to determine the category of a URL. If you want to suggest a new category for a URL use the feedback button to be redirected to the online WebGrade Feedback Form.

Check URL Category Submit Feedback

Screenshot 40 - Web Filtering Policies: WebGrade Database view

5.6.1 Enabling/Disabling the WebGrade Database

To enable or disable the WebGrade Database:

1. Navigate to **WebFilter Edition ► Web Filtering Policies ► WebGrade Database**.
2. Check or uncheck the checkbox from the **Enabled** column to enable or disable the database.



When the WebGrade Database is disabled, the Web Filtering Policies can no longer access the site categories.

3. Click **Save Settings**.

5.6.2 Enabling/Disabling Online Lookups for URLs

To enable or disable online lookups for URLs:

1. Navigate to **WebFilter Edition ► Web Filtering Policies ► WebGrade Database**.
2. Check or uncheck the **Enable online lookup for URLs not resolved by local database** checkbox to enable or disable this feature.



This option is enabled by default when the user updates the installation.

3. Click **Save Settings**.

5.6.3 Configuring WebGrade Database Updates

The **WebGrade Database Updates** area enables you to:

- » Configure whether the WebGrade Database should be updated automatically or by manually clicking **Update Now**.
- » Configure the frequency with which available updates should be installed
- » Configure if an email notification should be sent upon successful updating of the WebGrade Database

To configure settings for the WebGrade Database to update automatically:

1. Navigate to **WebFilter Edition ► Web Filtering Policies ► WebGrade Database**.
2. Check the **Manage WebGrade Local Database updates automatically** and update the time period within the **hours** field.
3. Select the **Send an email notification to the administrator on successfully updating the WebGrade Database** checkbox if required.
4. Click **Save Settings**.

5.6.4 Checking URL Categories

The **Check URL Category** area enables you to key in a URL and check for its category within your active local WebGrade database. If the category is not found or if the category listed in the local WebGrade database does not match with the website's category, you can report it for update.

To find out the category of a URL:

1. Navigate to **WebFilter Edition ► Web Filtering Policies ► WebGrade Database**.
2. Key in URL in the check URL field and click **Check URL Category**. The category in the active local WebGrade database is displayed beneath the URL field.

Reporting and/or Suggesting URL Categories

To report and/or suggest a wrongly categorized / uncategorized URL:

1. Click **Submit Feedback**. The **WebGrade customer feedback form** will be displayed in your browser.
2. Fill in the form and click **Submit**.

6.1 Introduction

The **WebSecurity Edition** node and its sub-nodes enable you to scan and restrict usage for various applications to users, groups or IP addresses on your network. The control policies include:

- » **Download Control Policies:** to control software downloads
- » **IM (Instant Messaging) Control Policies:** to control access and use of MSN / Microsoft Windows Live Messenger
- » **Virus Scanning Policies:** to configure which downloaded files should be scanned for viruses and spyware
- » **Anti-Phishing Engine:** to configure protection settings for network users against phishing sites.

6.2 Download Control Policies

The **Download Control Policies** node enables you to create policies per user(s), group(s) and/or IP(s) to manage file downloads based on file types. If the download of a file triggers a policy, GFI WebMonitor then uses the configured Download Control policy to determine what action to take. This may be one of the following actions:

- » Allow the file to be downloaded
- » Block the file from being downloaded and quarantine the downloaded file
- » Block the file from being downloaded and delete the downloaded file

	For allowed downloads, GFI WebMonitor then applies the configured Virus Scanning Policies.
	It is recommended that only one Download Control Policy is applied to a user, a group and/or IP address. In cases where more than one Download Control Policy is applied to the same user, group or IP, the top most policy takes priority over subsequent policies.

Download Control Policies

Use this page to configure download control policies that allow you to manage access to the internet per user, group, or IP. GFI WebMonitor checks each download against the policies configured below from top to bottom. The first policy to match is applied.

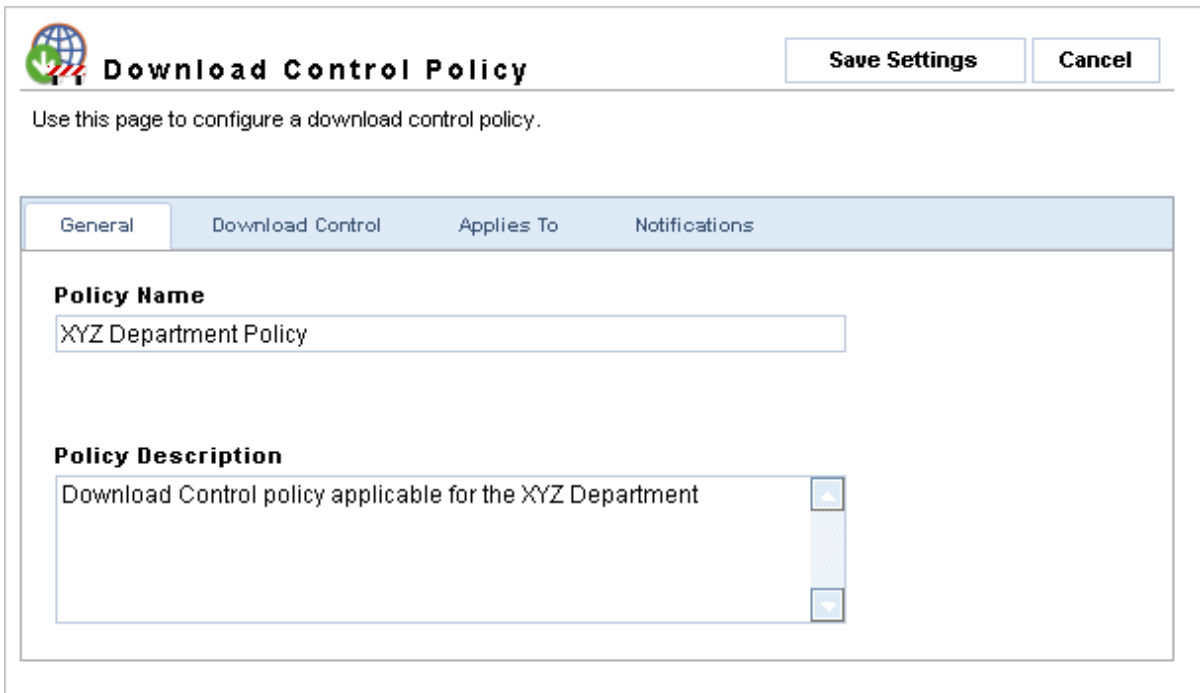
Policy Name	Applies To	Enabled		
XYZ Department Policy	192.168.99.50 bjones jdoe jsmith	<input checked="" type="checkbox"/>		
Default Download Control Policy	Applies to everyone	<input checked="" type="checkbox"/>		

Screenshot 41 - Download Control Policies view

6.2.1 Adding a Download Control Policy

To add a Download Control Policy:

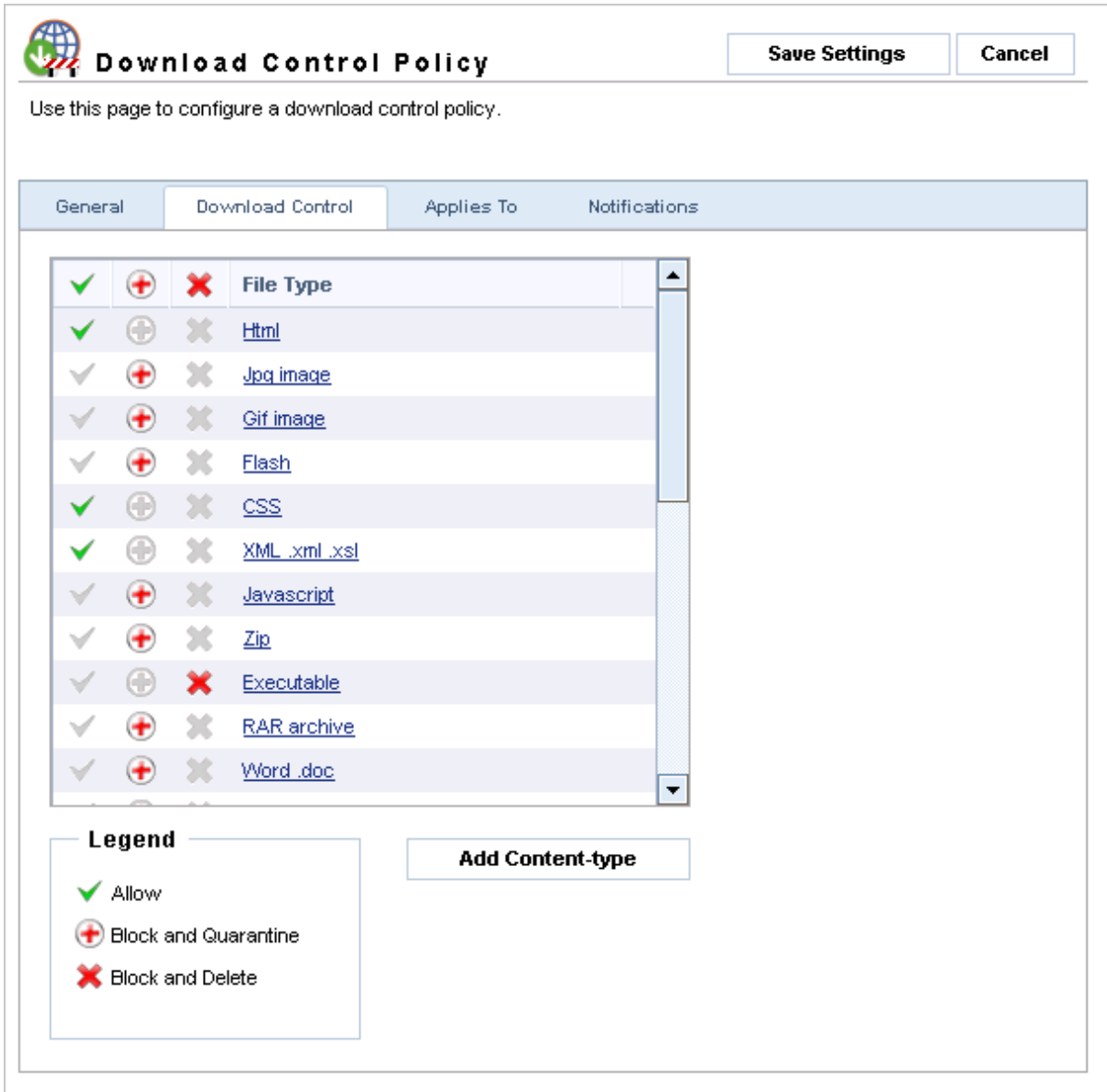
1. Navigate to **WebSecurity Edition ► Download Control Policies**.
2. Click **Add Policy**.



The screenshot shows a web interface for configuring a download control policy. At the top left is a globe icon with a red 'X' over it. The title is 'Download Control Policy'. To the right are 'Save Settings' and 'Cancel' buttons. Below the title is the instruction: 'Use this page to configure a download control policy.' There are four tabs: 'General', 'Download Control', 'Applies To', and 'Notifications'. The 'General' tab is selected. It contains two text input fields: 'Policy Name' with the value 'XYZ Department Policy' and 'Policy Description' with the value 'Download Control policy applicable for the XYZ Department'. The description field has a vertical scrollbar on the right side.

Screenshot 42 - Download Control Policies: General tab


3. In the **General** tab, key in a **Policy Name** and a **Policy Description**.




Screenshot 43 - Download Control Policies: Download Control tab

4. Select the **Download Control** tab and select the applicable action to be taken for each file type. The available options are:

- > Allow ✓
- > Block and Quarantine +
- > Block and Delete ✗

 The action can also be configured by clicking on a file type and setting the action from the **Change Action** dialog. A description about each file type is also provided.

 Click the **Add Content-type** button to add new file types. For more information, refer to the [Adding New Content-types](#) section in this chapter.

Download Control Policy Save Settings Cancel

Use this page to configure a download control policy.

General Download Control **Applies To** Notifications

If you need to create a policy that applies to all the users, you need to edit the settings in the Default Download Control Policy.

User Add

192.168.99.50	
bjones	
jdoe	
jsmith	

Screenshot 44 - Download Control Policies: Applies To tab

5. Select the **Applies To** tab and specify the **User**, **Group** and/or **IP** for whom the new policy applies, then click **Add**. Repeat for all the required users, groups and/or IP addresses.

- When keying in a **User**, specify the username in the format domain\user.
- When keying in an IP, you can use IP ranges (for example, “10.0.0.10-12” includes these IP addresses: “10.0.0.10”, “10.0.0.11” and “10.0.0.12”).



Download Control Policy

Save Settings

Cancel

Use this page to configure a download control policy.

General

Download Control

Applies To

Notifications

Notify the following administrators when the downloaded content infringes this policy.

Email Address

Add

No records available.

Send the following notification to the administrators

GFI WebMonitor has blocked access to download content that breaches a download control policy.

Notify the user performing the download when the downloaded content infringes this policy.

NOTE: The notification is sent only if the user performing the download is authenticated.

Send the following notification to the user performing the download

Your download has been blocked. The content breaches a GFI WebMonitor download control policy.

Screenshot 45 - Download Control Policies: Notifications tab


6. (Optional) Select the **Notifications** tab and define the notifications to send when a user infringes this policy. The available options are:

OPTION	DESCRIPTION
Notify the following administrators when the downloaded content infringes this policy	Select this option to send a notification to administrators. Add the administrator's email address and provide the body text of the notification email
Notify the user performing the download when the downloaded content infringes this policy	Select this option to send a notification to the user infringing this policy and provide the body text of the notification email

7. Click **Save Settings**. The new policy will now be listed in the main **Download Control Policies** view.

6.2.2 Editing a Download Control Policy

To edit a Download Control Policy:

1. Navigate to **WebSecurity Edition ► Download Control Policies**.
2. Click the **Edit** icon  next to the policy to edit.
3. Click **Save Settings**.


6.2.3 Enabling/Disabling a Download Control Policy

To enable or disable a Download Control Policy:

1. Navigate to **WebSecurity Edition ► Download Control Policies**.
2. Check or uncheck the checkbox from the **Enabled** column for the policy to enable or disable.
3. Click **Save Settings**.

6.2.4 Deleting a Download Control Policy



To delete a Download Control Policy:

1. Navigate to **WebSecurity Edition ► Download Control Policies**.
2. Click the **Delete** icon  next to the policy to delete.
3. Click **Save Settings**.

6.2.5 Default Download Control Policy

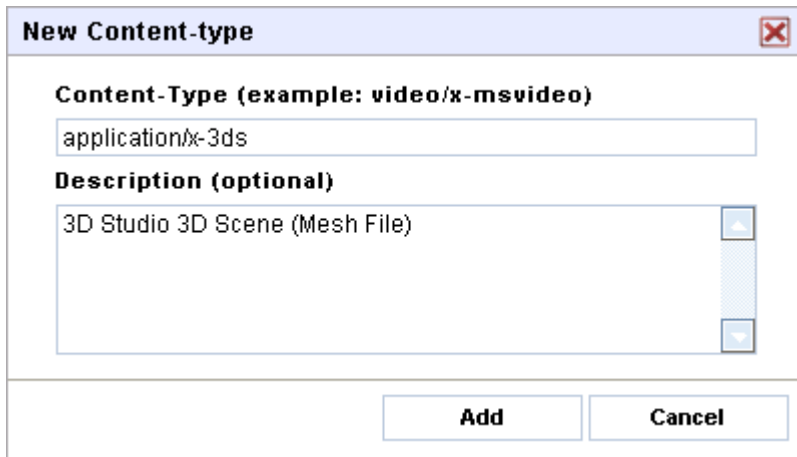
GFI WebMonitor - WebSecurity Edition ships with a default download control policy, which is configured to apply to all users. The policy name is listed as **Default Download Control Policy**.

This policy can be edited but it cannot be disabled or deleted. Refer to the [Editing a Download Control Policy](#) section in this chapter for information related to editing download control policies.

	All added Download Control Policies take priority over the Default Download Control Policy.
	Certain fields in the default policy cannot be edited. These include Policy Name, Policy Description and fields in the Applies To tab

6.2.6 Adding New Content-types

The **New Content-type** dialog enables you to create new definitions for file types, which are not yet in the predefined list.



New Content-type

Content-Type (example: video/x-msvideo)
application/x-3ds

Description (optional)
3D Studio 3D Scene (Mesh File)

Add **Cancel**

Screenshot 46 - Add new content type dialog

To create a new content-type:

1. Select the **Download Control** tab and click **Add Content-type** to view the **New Content-type** dialog.
2. Key in the content-type in the **Content-Type** field in the format type/subtype.
3. (Optional) Provide a description for the file type in the **Description** field.
4. Click **Add**.
5. Click **Save Settings**.

6.3 IM (Instant Messaging) Control Policies

The **IM Control Policies** node enables you to create policies per user(s), group(s) and/or IP(s) to control the use of MSN Messenger and Microsoft Windows Live Messenger. If a policy is breached, GFI WebMonitor then uses the configured IM Control policy to determine what action to take. This may be one of the following actions:

- Blocking all traffic related to MSN / Windows Live Messenger
- Allowing all traffic related to MSN / Windows Live Messenger

IM Control Policies Save Settings Cancel

Use this page to configure IM control policies for MSN / Windows Live Messenger

Add Policy

Policy Name	Applies To	Enabled		
XYZ Department Policy	192.168.99.50 bjohns jdoe jsmith	<input checked="" type="checkbox"/>		
Default IM Control Policy	Applies to everyone	<input checked="" type="checkbox"/>		

Screenshot 47 - IM Control Policies view

It is recommended that only one IM Control Policy is applied to a user, a group and/or IP address. In cases where more than one IM Control Policy is applied to the same user, group or IP, the top most policy takes priority over subsequent policies.

6.3.1 Adding an IM Control Policy

To add an IM Control Policy:

1. Navigate to **WebSecurity Edition ► IM Control Policies**.
2. Click **Add Policy**.

IM Control Policy Save Settings Cancel

Use this page to configure an IM control policy for MSN / Windows Live Messenger. Make sure that Windows Live Messenger(MSN) clients are passing via your proxy so GFI WebMonitor can apply desired actions. Windows Live Messenger(MSN) clients should use WEB(HTTP) protocol as the only way of communication.

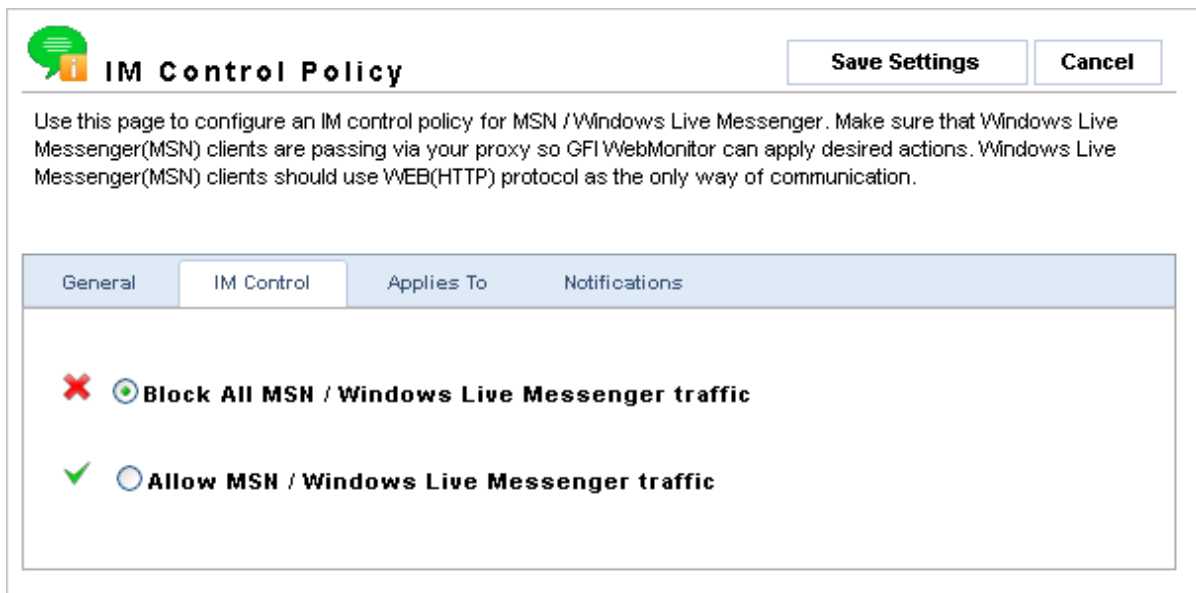
General | IM Control | Applies To | Notifications

Policy Name

Policy Description

Screenshot 48 - IM Control Policies: General tab

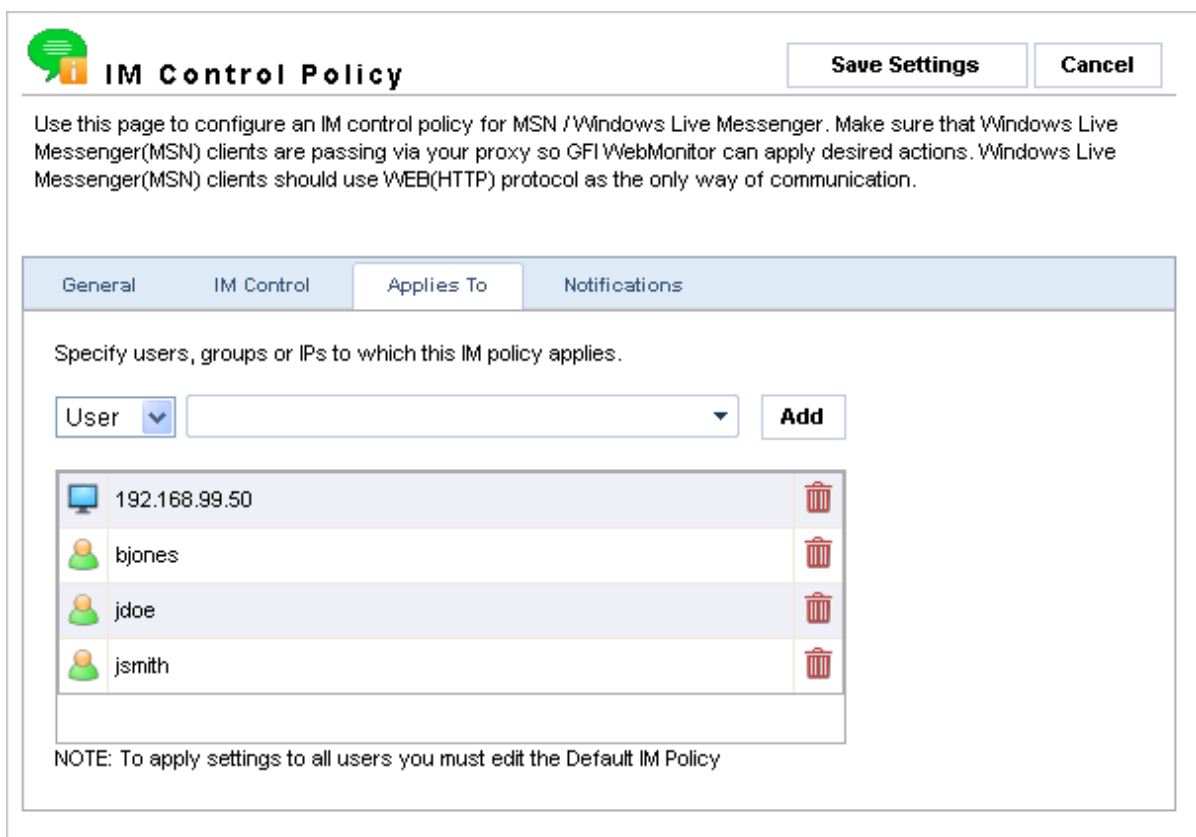
3. In the **General** tab provide a **Policy Name** and a **Policy Description**.



Screenshot 49 - IM Control Policies: IM Control tab


4. Select the **IM Control** tab and define the actions to take. The available options are:

- > Allow MSN / Windows Live Messenger traffic ✓
- > Block All MSN / Windows Live Messenger traffic ✗



Screenshot 50 - IM Control Policies: Applies To tab

5. Select the **Applies To** tab and specify the **User(s)**, **Group(s)** and/or **IP(s)** for whom the new policy applies and click **Add**. Repeat for all the required user(s), group(s) and/or IP(s).

 When keying in a **User**, specify the username in the format domain\user.



When keying in an IP, you can use IP ranges (for example, “10.0.0.10-12” includes these IP addresses: “10.0.0.10”, “10.0.0.11” and “10.0.0.12”).

IM Control Policy Save Settings Cancel

Use this page to configure an IM control policy for MSN / Windows Live Messenger. Make sure that Windows Live Messenger(MSN) clients are passing via your proxy so GFI WebMonitor can apply desired actions. Windows Live Messenger(MSN) clients should use WEB(HTTP) protocol as the only way of communication.

General **IM Control** **Applies To** **Notifications**

Notify the following administrators when this IM policy is breached

Email Address

Add

@ Administrator@krizz.local Remove

Send the following notification to the administrators

A user has breached the Default IM Control Policy. GFI WebMonitor blocked access to this content.

Notify the user breaching this IM policy.
NOTE: The notification is sent only if the user is authenticated.

Send the following notification to the user breaching the IM Control policy

WebMonitor has detected that you have breached an IM Control Policy. Please contact the administrator for more information.

Screenshot 51 - IM Control Policies: Notifications tab

6. (Optional) Select the **Notifications** tab and define the notifications to send when a user infringes this policy. The available options are:

OPTION	DESCRIPTION
Notify the following administrators when this IM policy is breached	Select this option to send a notification to administrators. Add the administrator’s email address and provide the body text of the notification email
Notify the user breaching this IM policy	Select this option to send a notification to the user infringing this policy and provide the body text of the notification email

7. Click **Save Settings**. The new policy will now be listed in the **IM Control Policies** view.

6.3.2 Editing an IM Control Policy

To edit an IM Control Policy:

1. Navigate to **WebSecurity Edition ► IM Control Policies**.
2. Click the **Edit** icon next to the policy to edit.

3. Click **Save Settings**.

6.3.3 Enabling/Disabling an IM Control Policy

To enable or disable an IM Control Policy:

1. Navigate to **WebSecurity Edition ► IM Control Policies**.
2. Check or uncheck the checkbox from the **Enabled** column for the policy to enable or disable.
3. Click **Save Settings**.

6.3.4 Deleting an IM Control Policy

To delete an IM Control Policy:

1. Navigate to **WebSecurity Edition ► IM Control Policies**.
2. Click the **Delete** icon  next to the policy to delete.
3. Click **Save Settings**.

6.3.5 Default IM Control Policy

GFI WebMonitor - WebSecurity Edition ships with a default instant messaging control policy, which is configured to apply to all users. The policy name is listed as **Default IM Control Policy**.

This policy can be edited but it cannot be disabled or deleted. Refer to the [Editing an IM Control Policy](#) section in this chapter for information related to editing download control policies.



All added IM Control Policies take priority over the **Default IM Control Policy**.



Certain fields in the default policy cannot be edited. These include **Policy Name**, **Policy Description** and fields in the **Applies To** tab.

6.4 Virus Scanning Policies

The **Virus Scanning Policies** node enables you to create policies per user(s), group(s) and/or IP(s) to manage virus scanning of files based on file types. If the download of an infected file triggers a policy, GFI WebMonitor then uses the configured Virus Scanning policy to determine what action to take. This may be one of the following actions:

- » Issue a warning, but still Allow the file to be downloaded
- » Block the file from being downloaded and quarantine the downloaded file
- » Block the file from being downloaded and delete the downloaded file

GFI WebMonitor scans the downloaded files with any of the supported virus scanners. On the user's machine, GFI WebMonitor displays the download progress, the virus scanning status and progress as well as the results.



It is recommended that only one Virus Scanning Policy is applied to a user, a group and/or IP address. In cases where more than one Virus Scanning Policy is applied to the same user, group or IP, the top most policy takes priority over subsequent policies.

Virus Scanning Policies Save Settings Cancel

Use this page to configure virus scanning policies to specify which downloaded files should be scanned for viruses and spyware. The policies can be configured per user, group, or IP, so that you can, for example, exclude certain power users from virus scanning. GFI WebMonitor checks each download against the policies configured below from top to bottom. The first policy to match is applied.

Add Policy

Policy Name	Applies To	Enabled		
XYZ Department Policy	192.168.99.50 bjohnes jdoe jsmith	<input checked="" type="checkbox"/>		
Default Virus Scanning Policy	Applies to everyone	<input checked="" type="checkbox"/>		

Screenshot 52 - Virus Scanning Policies view

6.4.1 Adding a Virus Scanning Policy

To add a Virus Scanning Policy:

1. Navigate to **WebSecurity Edition ► Virus Scanning Policies**.
2. Click **Add Policy**.

Virus Scanning Policy Save Settings Cancel

Use this page to configure a virus scanning policy.

General **Virus Scanning** Applies To Notifications


Policy Name
XYZ Department Policy


Policy Description
Virus Scanning policy applicable for the XYZ Department

Screenshot 53 - Virus Scanning Policies: General tab

3. In the **General** tab provide a **Policy Name** and a **Policy Description**.
4. Select the **Virus Scanning** tab and select the applicable action to be taken for each file type. The available options are:
 - > Warn and Allow
 - > Block and Quarantine

> Block and Delete ✖

5. Under the **Scan With** column, select the **Display download progress and status icon**  to display a notification window to the user during file download.



Virus Detected Action	File Type	Scan With
	Html	
	Jpg image	
	Gif image	
	Flash	
	CSS	
	XML .xml .xsl	
	Javascript	
	Zip	
	Executable	
	RAR archive	



Legend

- Warn and Allow
- Block and Quarantine
- Block and Delete
- Display download progress and status
- Scan with BitDefender
- Scan with Kaspersky
- Scan with Norman

Add Content-type

Screenshot 54 - Virus Scanning Policies: Virus Scanning tab

6. Under the **Scan With** columns, select the anti-virus engine(s) to scan the downloaded files with.

-  The action can also be configured by clicking on a file type and setting the action from the **Select Virus Scanners and Action** dialog. A description about each file type is also provided.
-  Click the **Add Content-type** button to add new file types. For more information, refer to the [Adding New Content-types](#) section in this chapter.

Virus Scanning Policy Save Settings Cancel

Use this page to configure a virus scanning policy.

General Virus Scanning **Applies To** Notifications

If you need to create a policy that applies to all the users, you need to edit the settings in the Default Virus Scanning Policy.

User

	192.168.99.50	
	bjones	
	jdoe	
	jsmith	

Screenshot 55 - Virus Scanning Policies: Applies To tab

7. Select the **Applies To** tab and specify the **User**, **Group** and/or **IP** for whom the new policy applies, then click **Add**. Repeat for all the required users, groups and/or IPs.

- When keying in a **User**, specify the username in the format domain\user.
- When keying in an **IP**, you can use IP ranges (for example, “10.0.0.10-12” includes these IP addresses: “10.0.0.10”, “10.0.0.11” and “10.0.0.12”).

Screenshot 56 - Virus Scanning Policies: Notifications tab


8. (Optional) Select the **Notifications** tab and define the notifications to send when a user infringes this policy. The available options are:

OPTION	DESCRIPTION
Notify the following administrators when the downloaded content infringes this policy	Select this option to send a notification to administrators. Add the administrator's email address and provide the body text of the notification email
Notify the user performing the download when the downloaded content infringes this policy	Select this option to send a notification to the user infringing this policy and provide the body text of the notification email

9. Click **Save Settings**. The new policy will now be listed in the main **Virus Scanning Policies** view.

6.4.2 Editing a Virus Scanning Policy

To edit a Virus Scanning Policy:

1. Navigate to **WebSecurity Edition ► Virus Scanning Policies**.
2. Click the **Edit** icon  next to the policy to edit.
3. Click **Save Settings**.


6.4.3 Enabling/Disabling a Virus Scanning Policy

To enable or disable a Virus Scanning Policy:

1. Navigate to **WebSecurity Edition ► Virus Scanning Policies**.
2. Check or uncheck the checkbox from the **Enabled** column for the policy to enable or disable.
3. Click **Save Settings**.

6.4.4 Deleting a Virus Scanning Policy

To delete a Virus Scanning Policy:

1. Navigate to **WebSecurity Edition ► Virus Scanning Policies**.
2. Click the **Delete** icon  next to the policy to delete.
3. Click **Save Settings**.

6.4.5 Default Virus Scanning Policy

GFI WebMonitor WebSecurity Edition ships with a default virus scanning policy, which is configured to apply to all users. The policy name is listed as **Default Virus Scanning Policy**.

This policy can be edited but it cannot be disabled or deleted. Refer to the [Editing a Virus Scanning Policy](#) section in this chapter for information related to editing virus-scanning policies.



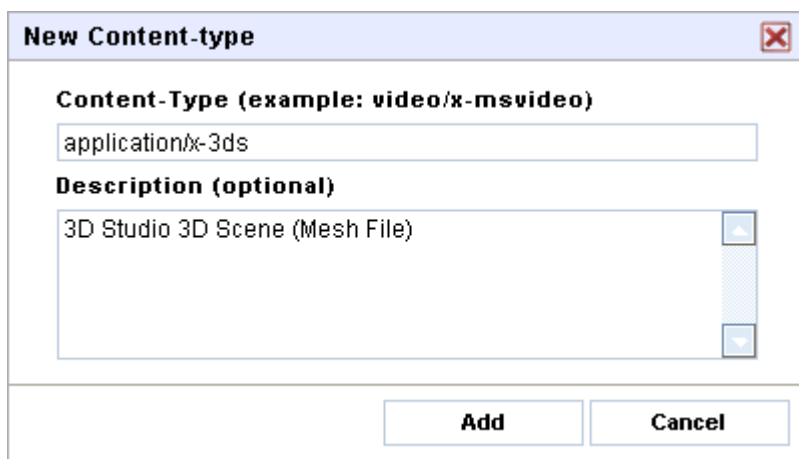
All added Virus Scanning Policies take priority over the Default Virus Scanning Policy.



Certain fields in the default policy cannot be edited. These include **Policy Name**, **Policy Description** and fields in the **Applies To** tab.

6.4.6 Adding New Content-types

The **New Content-type** dialog enables you create new definitions for file types, which are not yet in the predefined list.



Screenshot 57 - Add new content type dialog

To create a new content-type:

1. Select the **Virus Scanning** tab and click **Add Content-type** to view the **New Content-type** dialog.
2. Key in the content-type in the **Content-Type** field in the format type/subtype.
3. (Optional) Provide a description for the file type in the **Description** field.

4. Click **Add**.
5. Click **Save Settings**.

6.5 Virus & Spyware Protection

The **Virus & Spyware Protection** node enables you to:

- » Enable or disable one or more of the supported anti-virus scanning engines
- » View the anti-virus scanning engine status, version and license details
- » Configure anti-virus updates for each of the anti-virus scanning engines

Use this page to enable/disable the virus scanning engines and to check their licensing status.

Engine	Enabled	Status
BitDefender Anti-Virus	<input checked="" type="checkbox"/>	Licensed
Kaspersky Anti-Virus	<input checked="" type="checkbox"/>	Licensed
Norman Anti-Virus	<input checked="" type="checkbox"/>	Licensed

Screenshot 58 - Virus & Spyware Protection view

6.5.1 Enabling/Disabling the Scanning Engines

To enable or disable one or more of the anti-virus scanning engines:

1. Navigate to **WebSecurity Edition ► Virus Scanning Policies ► Virus & Spyware Protection**.
2. Check or uncheck the checkbox from the **Enabled** column to enable or disable a scanning engine.



When an anti-virus scanning engine is disabled, GFI WebMonitor can no longer scan files using that disabled engine.

3. Click **Save Settings**.

6.5.2 Configuring Anti-Virus Updates

The **Anti-Virus Updates** area for each one of the supported anti-virus scanning engines enables you to:

- » Configure whether the scanning engine should be updated automatically or by manually clicking **Update Now**
- » Configure the frequency with which available updates should be installed
- » Configure if an email notification should be sent upon successful updating of the scanning engine

BitDefender Anti-Virus Save Settings Cancel

Use this page to check the licensing status for the BitDefender Anti-Virus, and to configure automatic updates, and notification settings.

Anti-virus Engine Status and Version	Active. AVCORE v2.1 Windows/i386 11.0.0.42 (Aug 31 2010). Signatures: 5994744 (2010-10-14 07:41)
Anti-Virus Engine License Status	Licensed.

Anti-Virus Updates

Manage anti-virus updates automatically

Check for anti-virus updates, and if available install them, every: hours

Send an email notification to the administrator on successfully updating the anti-virus.
NOTE: If an anti-virus update fails, an email notification is always sent to the administrator.

Anti-virus last updated on: Update Now

Screenshot 59 - BitDefender Anti-Virus view

Norman Anti-Virus Save Settings Cancel

Use this page to check the licensing status for the Norman Anti-Virus, and to configure automatic updates, and notification settings.

Anti-virus Engine Status and Version	Active. Version: 6.6.7(10) Signatures:7683167. (2010-10-13 06:22)
Anti-Virus Engine License Status	Licensed.

Anti-Virus Updates

Manage anti-virus updates automatically


Check for anti-virus updates, and if available install them, every: hours


Send an email notification to the administrator on successfully updating the anti-virus.
NOTE: If an anti-virus update fails, an email notification is always sent to the administrator.

Anti-virus last updated on: Update Now

Screenshot 60 - Norman Anti-Virus view

To configure settings for any of the anti-virus scanning engines to update automatically:

1. Navigate to **WebSecurity Edition ► Virus Scanning Policies ► Virus & Spyware Protection** and click the **Edit** icon  next to the anti-virus scanning engine to edit.

 Optionally, move the mouse pointer over the Anti-Virus Engine name and click once

2. Check the **Manage anti-virus updates automatically** and update the time period within the **hours** field.

3. Select the **Send an email notification to the administrator on successfully updating the anti-virus** checkbox if required.

4. Click **Save Settings**.

Configuring Kaspersky Virus-Scanning Engine Options

The Kaspersky anti-virus scanning engine enables you to state whether the actions specified in the Virus Scanning Policies should also be used when files are identified as:

- » Suspicious
- » Corrupted (that is, files that cannot be scanned since the file format is corrupted, for example, corrupted CAB files)
- » Hidden (that is, files that cannot be scanned since the contents are protected, for example, password protected ZIP files)

Anti-virus Engine Status and Version	Active. Version: 8.0.2.45, Signatures: 4167806. (2010-10-14 07:43)
Anti-Virus Engine License Status	Licensed.

Anti-Virus Updates

Manage anti-virus updates automatically

Check for anti-virus updates, and if available install them, every: hours

Send an email notification to the administrator on successfully updating the anti-virus.
NOTE: If an anti-virus update fails, an email notification is always sent to the administrator.

Anti-virus last updated on:

Virus-Scanning Engine Options

Trigger configured action also for files identified as:

Suspicious

Corrupted (Files that cannot be scanned since the file format is corrupted, for example, corrupted CAB files.)

Hidden (Files that cannot be scanned since the contents are protected, for example, password protected ZIP files.)

Screenshot 61 - Kaspersky Anti-Virus view

1. Navigate to **WebSecurity Edition ► Virus Scanning Policies ► Virus & Spyware Protection ► Kaspersky Anti-Virus.**
2. Check or uncheck the **Suspicious**, **Corrupted** or **Hidden** checkboxes to enable or disable the relevant **Virus Scanning Policies** actions for files identified as Suspicious, Corrupted or Hidden.
3. Click **Save Settings**.

6.6 Anti-Phishing Engine

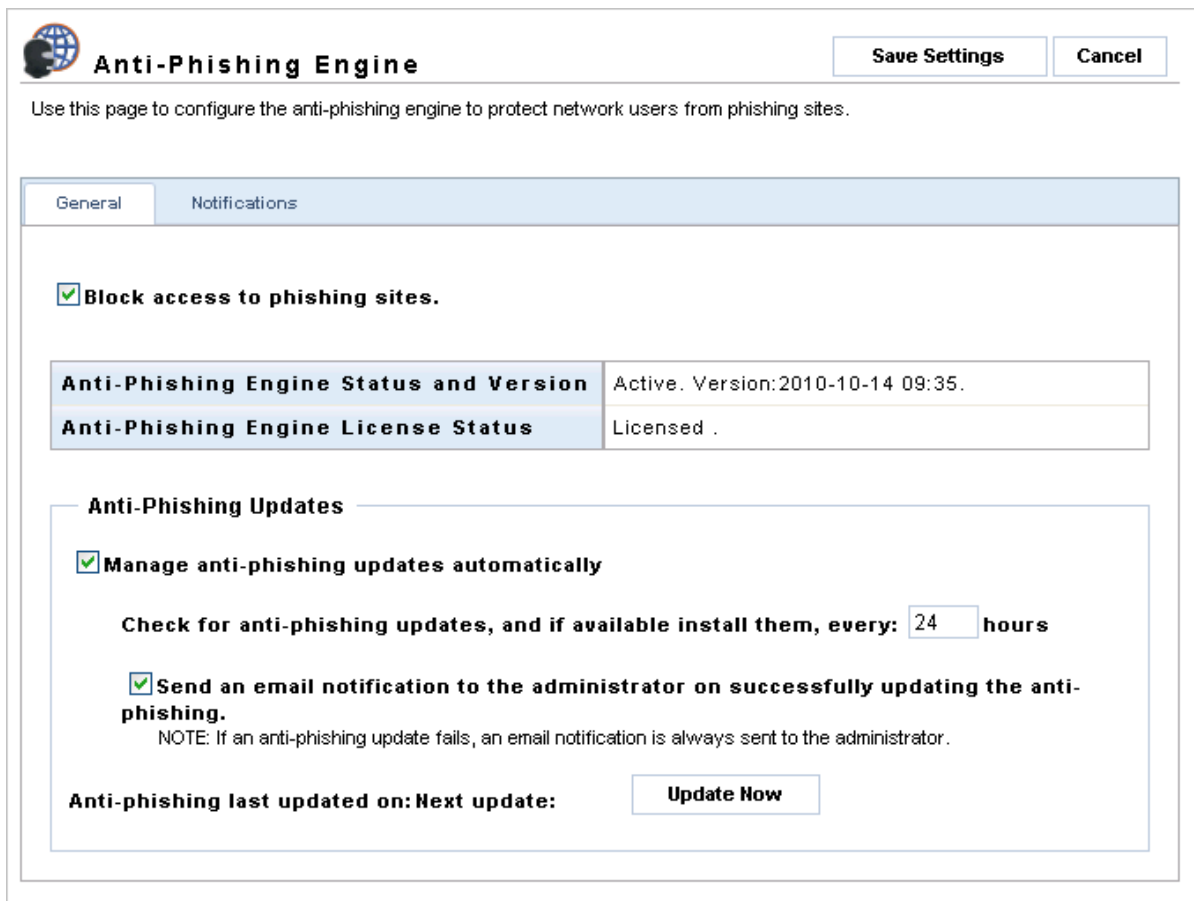
The **Anti-Phishing Engine** node enables you to:

- › Enable or disable anti-phishing monitoring
- › View the anti-phishing database status, version and license details
- › Configure anti-phishing database updates

6.6.1 Enabling/Disabling the Anti-Phishing Engine

To enable or disable the Anti-Phishing Engine:

1. Navigate to **WebSecurity Edition ► Anti-Phishing Engine**.



The screenshot shows the 'Anti-Phishing Engine' configuration page. At the top, there is a title bar with a globe icon and the text 'Anti-Phishing Engine'. To the right of the title bar are two buttons: 'Save Settings' and 'Cancel'. Below the title bar is a descriptive sentence: 'Use this page to configure the anti-phishing engine to protect network users from phishing sites.' The main content area has two tabs: 'General' (selected) and 'Notifications'. Under the 'General' tab, there is a checkbox labeled 'Block access to phishing sites.' which is checked. Below this is a table with two rows: 'Anti-Phishing Engine Status and Version' with the value 'Active. Version:2010-10-14 09:35.' and 'Anti-Phishing Engine License Status' with the value 'Licensed.'. Below the table is a section titled 'Anti-Phishing Updates' containing a checked checkbox 'Manage anti-phishing updates automatically'. Underneath, it says 'Check for anti-phishing updates, and if available install them, every: 24 hours'. There is another checked checkbox 'Send an email notification to the administrator on successfully updating the anti-phishing.' followed by a note: 'NOTE: If an anti-phishing update fails, an email notification is always sent to the administrator.' At the bottom of this section, it says 'Anti-phishing last updated on: Next update:' followed by an 'Update Now' button.

Screenshot 62 - Anti-Phishing Engine: General tab

2. Click the **General** tab.
3. Check or uncheck the **Block access to phishing sites** checkbox to enable or disable anti-phishing features.



When the anti-phishing engine is disabled, GFI WebMonitor can no longer block phishing sites.

4. Click **Save Settings**.

6.6.2 Configuring Anti-Phishing Database Updates

The **Anti-Phishing Updates** area enables you to:

- » Configure whether the anti-phishing engine should be updated automatically or by manually clicking **Update Now**
- » Configure the frequency with which available updates should be installed
- » Configure if an email notification should be sent upon successful updating of the anti-phishing engine

To configure settings for the anti-phishing engine to update automatically:

1. Navigate to **WebSecurity Edition ► Anti-Phishing Engine**.
2. In the **General** tab check the **Manage anti-phishing updates automatically** and update the time period within the **hours** field.
3. Select the **Send an email notification to the administrator on successfully updating the anti-phishing** checkbox if required.
4. Click **Save Settings**.

6.6.3 Configuring Phishing Notifications

The **Notifications** tab in **Anti-Phishing Engine** node enables you to specify whether email notifications are to be sent to administrators and / or to users when an accessed site is identified as a phishing site.

To configure phishing notifications:

1. Navigate to **WebSecurity Edition ► Anti-Phishing Engine**.

Anti-Phishing Engine Save Settings Cancel

Use this page to configure the anti-phishing engine to protect network users from phishing sites.

General **Notifications**

Notify the following administrators when the site accessed is a known phishing site.

Email Address

Add

No records available.

Send the following notification to the administrators

GFI WebMonitor blocked access to a known phishing site.

Notify the user accessing the site if the site accessed is a known phishing site.

NOTE: The notification is sent only if the user performing the download is authenticated.

Send the following notification to the user accessing the site

GFI WebMonitor protected you from accessing a known phishing site.

Screenshot 63 - Anti-Phishing Engine: Notifications tab

2. Select the **Notifications** tab and define the notifications to send when a user infringes this policy. The available options are:

OPTION	DESCRIPTION
Notify the following administrators when the site accessed is a known phishing site	Select this option to send a notification to administrators. Add the administrator's email address and provide the body text of the notification email.
Notify the user accessing the site if the site accessed is a known phishing site	Select this option to send a notification to the user infringing this policy and provide the body text of the notification email

3. Click **Save Settings**.

7 Configuring GFI WebMonitor

7.1 Introduction

The **Configuration** node and its sub-nodes enable you to configure a default set of parameters used by the WebFilter and WebSecurity editions. The configuration parameters include:

PARAMETERS	DESCRIPTION
Administrative Access Control	To configure who can access GFI WebMonitor web interface for configuration and monitoring
Notifications	To configure alerting options for email notifications on important events and licensing
General Settings	To configure the data retention, downloaded cache, temporary whitelist policies and number of records to be displayed per page
Reporting	Configure the database settings for reporting



When configuring the options mentioned in this section it is important to click **Save Settings** in order to confirm the changes before leaving the page.

7.2 Administrative Access Control

The **Administrative Access Control** node enables you to list the user(s) and IP(s), which are allowed to access the GFI WebMonitor application (that is, by keying in the URL <http://monitor.isa> in their web browser) from their machine. Specified users are allowed access to GFI WebMonitor only if their username has been authenticated.

7.2.1 Adding Users/IP addresses to the Access Permissions List

IP	Add
127.0.0.1	
192.168.99.50	
bjones	
jdoe	
jsmith	

Screenshot 64 - Configuration: Administrative Access Control view

To add a user and/or IP to the access permissions list:

1. Navigate to **Configuration ► Administrative Access Control**.
2. Specify the **User** or **IP**, who is allowed to access the GFI WebMonitor application from his machine and click **Add**. Repeat for all the required user(s) and/or IP (s).



When keying in a **User**, specify the username in the format domain\user.




IP ranges are not supported.

3. Click **Save Settings**.

7.2.2 Deleting Users/IP Addresses From the Access Permissions List

To delete a user and/or IP from the access permissions list:

1. Navigate to **Configuration ► Administrative Access Control**.
2. Click the **Delete** icon  next to the user/IP to delete.
3. Click **Save Settings**.

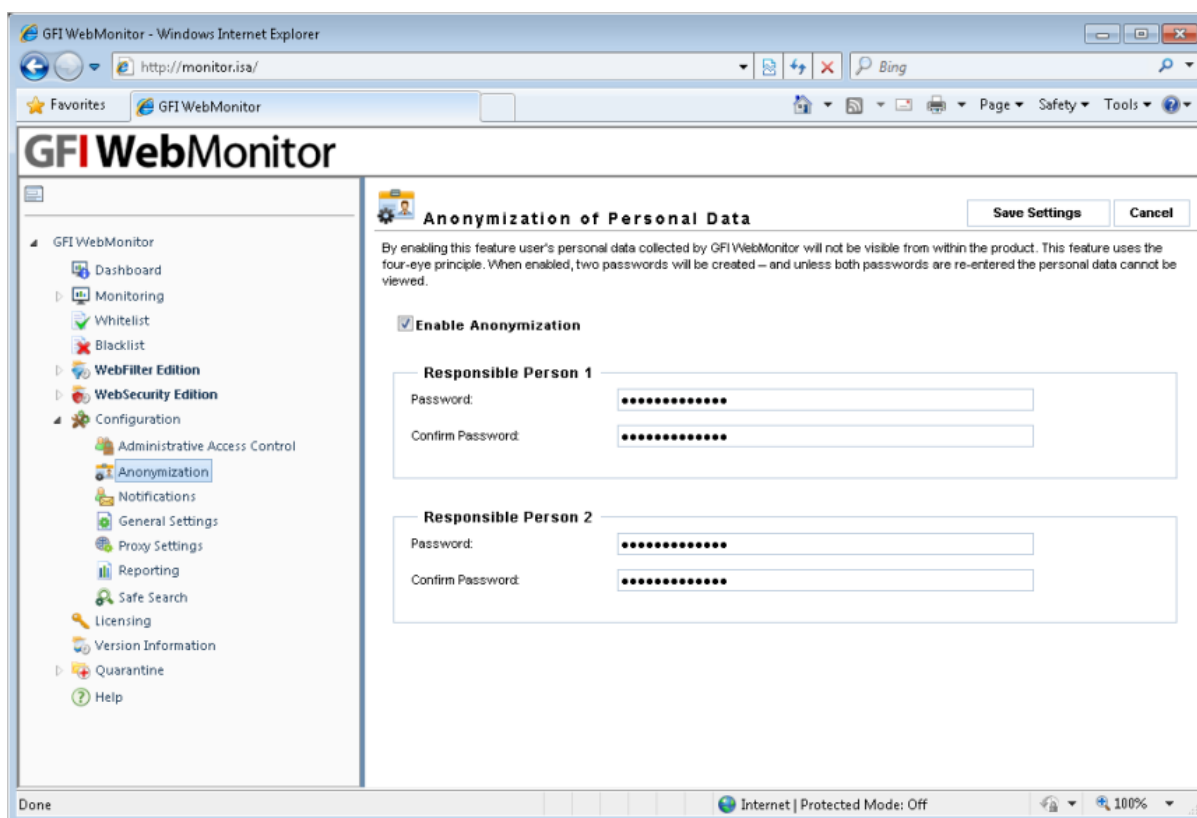
7.3 Anonymization

The Anonymization node enables masking private user data in accordance with European privacy and data protection laws. If enabled, GFI WebMonitor:

- › Cloaks personal data (User name and IP) so that it can no longer be viewed from the Monitoring Reports section or ReportPack.
- › Enables a validation process requiring two passwords from two different users.
- › Masks any features in the User Interface that provide access to private user information.

7.3.1 Enabling Anonymization

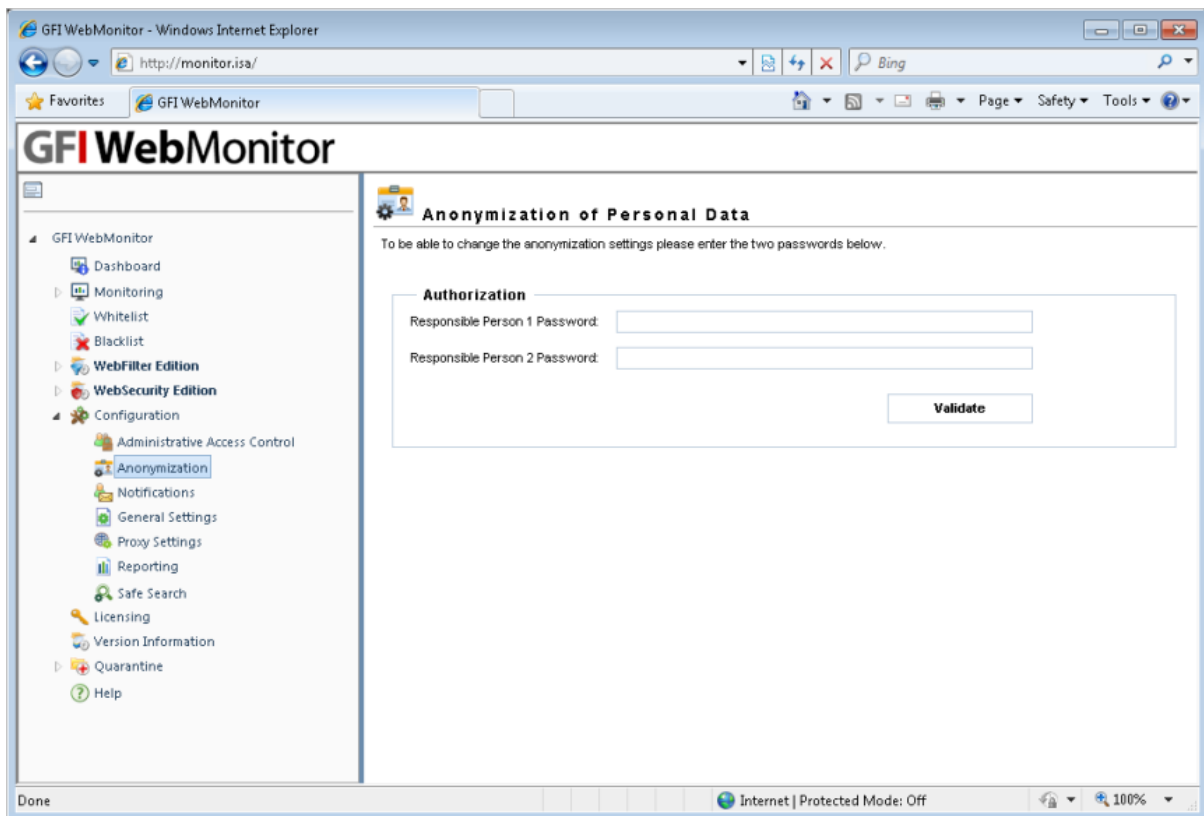
1. Navigate to **Configuration ► Anonymization**.
2. Click **Enable Anonymization** checkbox.
3. Enter the passwords for **Responsible Person 1** and **Responsible Person 2**.
4. Click **Save Settings**.



Screenshot 65 - Enabling Anonymization

7.3.2 Disabling Anonymization

1. Navigate to **Configuration ► Anonymization**.
2. Enter the password for **Responsible Person 1** and **Responsible Person 2**.
3. Click **Validate**.
4. Uncheck the **Enable Anonymization** checkbox
5. Click **Save Settings**.



Screenshot 66 - Disabling Anonymization

7.4 Notifications

The **Notifications** node enables you to specify from where and to whom are important administrative notifications sent. Such emails are sent on important events including:

- » Items being blocked or quarantined
- » WebGrade Database and/or anti-virus signature update failures
- » WebGrade Database and/or anti-virus signature update success
- » Approaching expiry of WebGrade Database and/or to update anti-virus signature licenses.

7.4.1 Configuring the Sender of Administrative Notifications

To configure the sender:

1. Navigate to **Configuration ► Notifications**.
2. In the **Send administrative emails using the following settings** area, key in the sender's email address, the SMTP server and SMTP port.
3. Click **Save Settings**.

7.4.2 Configuring the Recipients of Administrative Notifications

Notifications Save Settings Cancel

Use this page to specify the settings GFI WebMonitor should use to send important administrative notifications, such as, block and quarantine notifications, and warnings when anti-virus definition files fail to update or the update licences are approaching expiry.

Send administrative emails using the following settings

From email address
WebMonitor@127.0.0.1

SMTP Server **SMTP Port**
127.0.0.1 25

Send administrative emails to the following recipients

Email Address
[Empty field] Add

@ Administrator@127.0.0.1 Delete


Screenshot 67 - Configuration: Notifications view

To add recipients to whom notifications are sent:

1. Navigate to **Configuration ► Notifications**.
2. In the **Email Address** field specify the email address(es) of the recipient(s) and click **Add**. Repeat for all the required recipients.
3. Click **Save Settings**.

7.4.3 Deleting Email Recipients

To delete recipients to whom notifications are sent:

1. Navigate to **Configuration ► Notifications**.
2. Click the **Delete** icon  next to the email address to delete.
3. Click **Save Settings**.

7.5 General Settings

The **General Settings** node enables you to configure generic settings. The settings include:

- » The number of days to keep browsing data in the database
- » The number of hours to keep downloaded files in the GFI WebMonitor cache
- » The number of hours a site is kept in the temporary whitelist after it has been approved from the quarantine

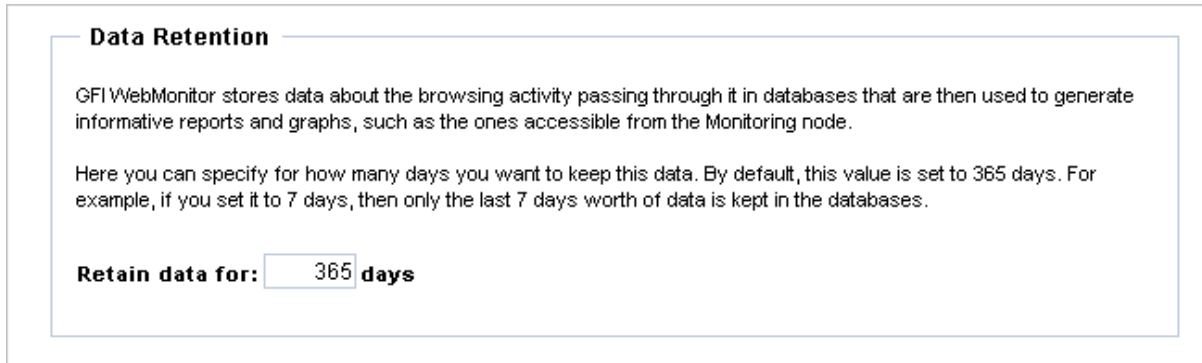
- » The number of records per page, shown for every report
- » The list of IP addresses of proxy servers on the same network
- » The language in which messages are displayed on users' machines.

7.5.1 Data Retention

The **Data Retention** area enables you to configure a length of time (measured in days) for keeping browsing activity data in the GFI WebMonitor databases. This data is used for monitoring and reporting.

To configure for how long browsing activity data is kept:

1. Navigate to **Configuration ► General Settings**.



Screenshot 68 - Configuration: General Settings view - Data Retention

2. From the **Data Retention** area, key in the number of days in the **Retain data for:** field.
3. Click **Save Settings**.



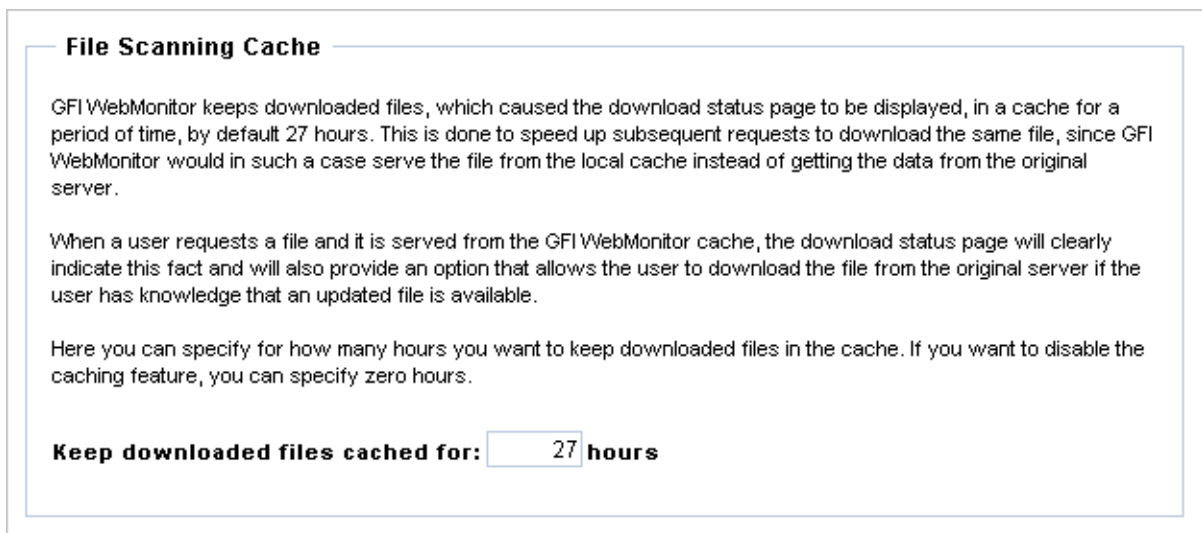
The default value is set to 365 days.

7.5.2 File Scanning Cache

The **File Scanning Cache** area enables you to configure for how long (in hours) downloaded files will be kept in a local cache. Keeping these files in the cache will speed up subsequent requests for the same file.



To configure for how long downloaded files are kept:

1. Navigate to **Configuration ► General Settings**.



2. From the **File Scanning Cache** area, key in the number of hours in the **Keep downloaded files cached for x hours** field.

3. Click **Save Settings**.

	The default value is set to 27 hours.
	To disable the caching feature set the value to zero hours.

7.5.3 Temporary Whitelist

The **Temporary Whitelist** area enables you to configure the length of time (measured in hours) items approved from quarantine will be kept in the Temporary Whitelist. This is the amount of time during which the approved URL is accessible.

To configure for how long approved quarantined items are accessible:

1. Navigate to **Configuration ► General Settings**.

Temporary Whitelist

When you approve an item from the GFI WebMonitor quarantine, the URL is automatically added to the temporary whitelist feature. In this way, the specified user has a set amount of time during which the URL is accessible and will not trigger any of the GFI WebMonitor policies configured.

By default, items approved from the quarantine are added to the temporary whitelist with the time setting set to 52 hours.

Here you can specify the default amount of hours you want to set when approving new items from the quarantine.

By default, approve items for: **hours**

Screenshot 70 - Configuration: General Settings view - Temporary Whitelist

2. From the **Temporary Whitelist** area, key in the number of hours in the **By default, approve items for:** field.

3. Click **Save Settings**.

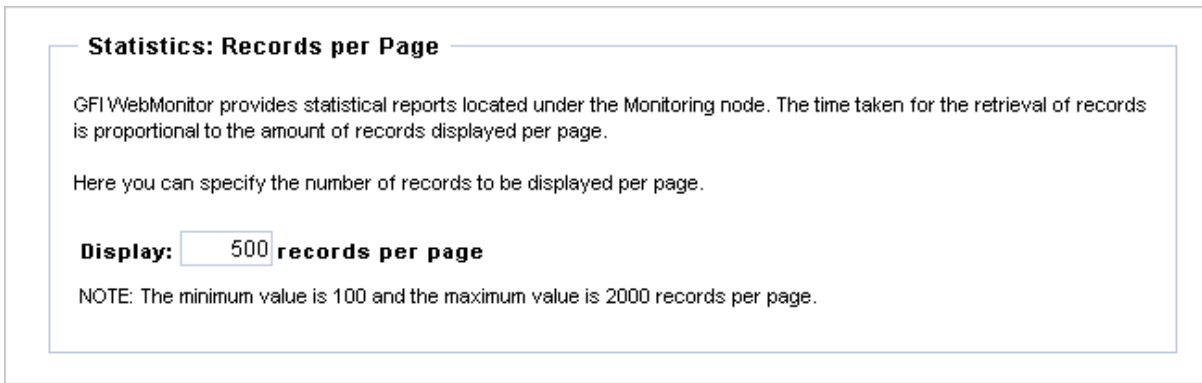
7.5.4 Statistics: Records per Page

The **Statistics: Records per Page** area enables you to configure the number of records to display per page for reports generated in the **Monitoring** node.

	This setting does not apply for the Top Categories report.
---	---

To configure the number of records to be displayed per page:

1. Navigate to **Configuration ► General Settings**.



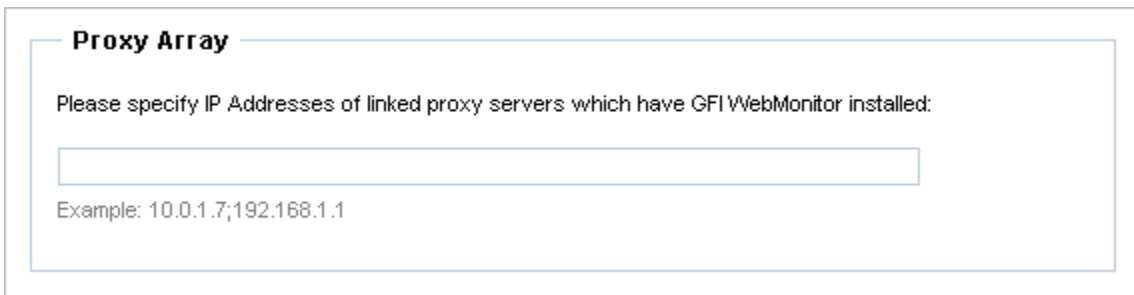
Screenshot 71 - Configuration: General Settings view - Statistics: Records per Page

2. From the **Statistics: Records per Page** area, key in the number of records in the **Display x records per page** field.

3. Click **Save Settings**.

7.5.5 Proxy Array

1. Navigate to **Configuration ► General Settings**.



Screenshot 72 - Configuration: General Settings view - Proxy Array

2. In the **Proxy Array** area, key in the IP Addresses of linked proxy servers which have GFI WebMonitor installed.

3. Click **Save Settings**.

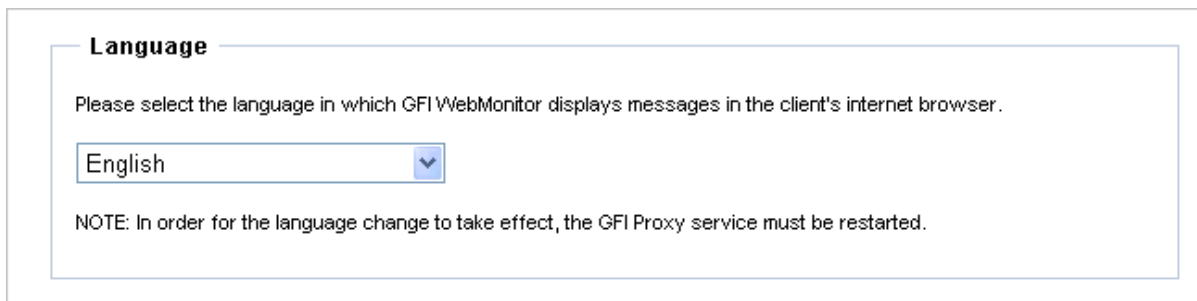
7.5.6 Language

The **Language** area enables you to configure the language in which GFI WebMonitor displays messages on the user's machines. Messages from GFI WebMonitor include:

- » Download status windows
- » URL blocking notifications
- » HTTPS Scanning Warning Page

To configure the language of the GFI WebMonitor messages:

1. Navigate to **Configuration ► General Settings**.



Screenshot 73 - Configuration: General Settings view - Language

2. From the **Language** area, select the language from the drop-down list, in which GFI WebMonitor displays messages on the user's machines.
3. Click **Save Settings**.

7.6 Reporting

The **Reporting** node enables you to store data on an existing database for statistical information. Use GFI WebMonitor ReportPack to view and analyze stored information. In this section, you will find information about:

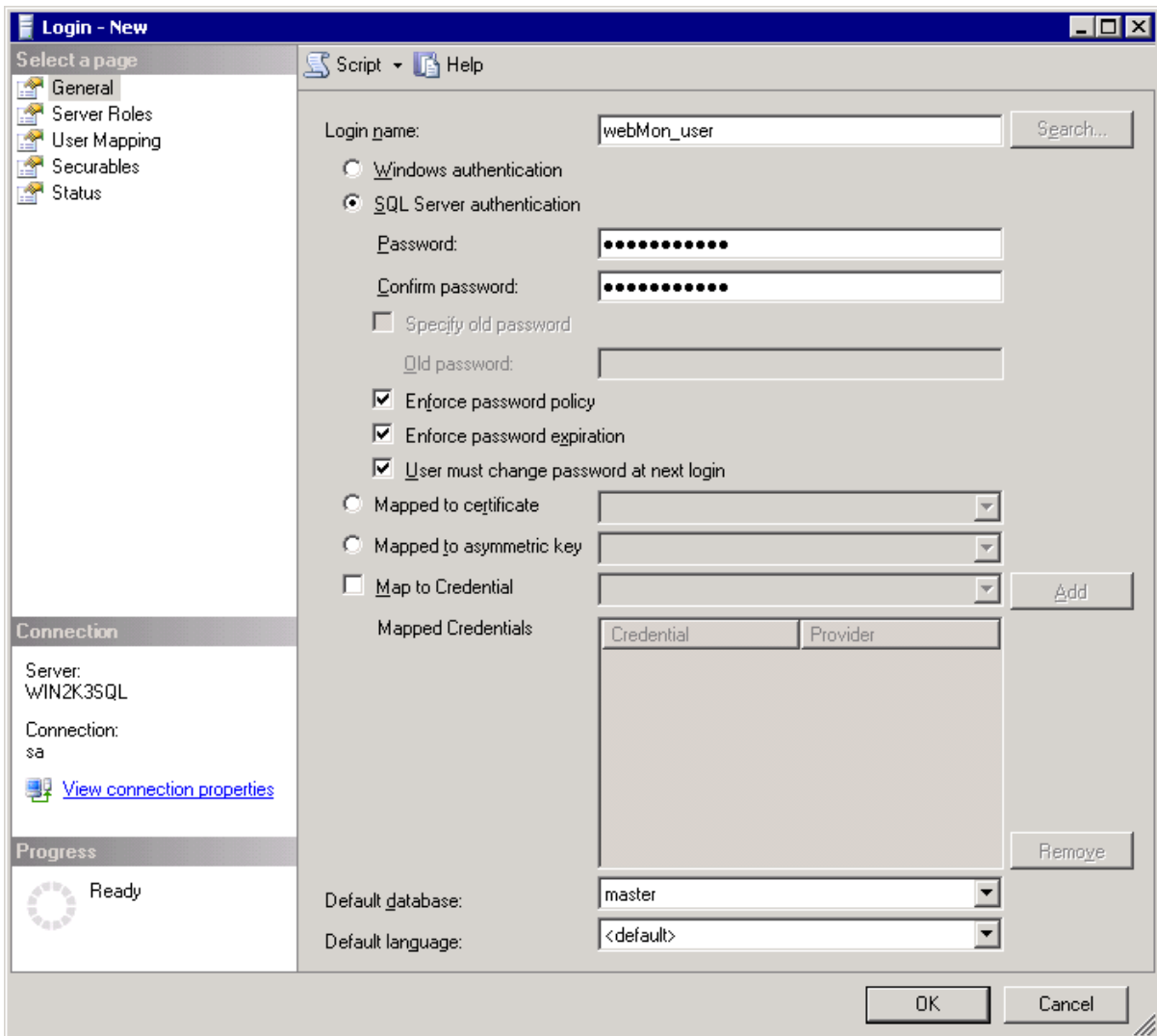
- » Reporting requirements
- » How to enable or disable information gathering
- » Configuring reporting options.

7.6.1 Reporting Requirements

Before enabling reporting, create a blank database in an SQL environment. On enabling reporting, the database structure is automatically configured by GFI WebMonitor.

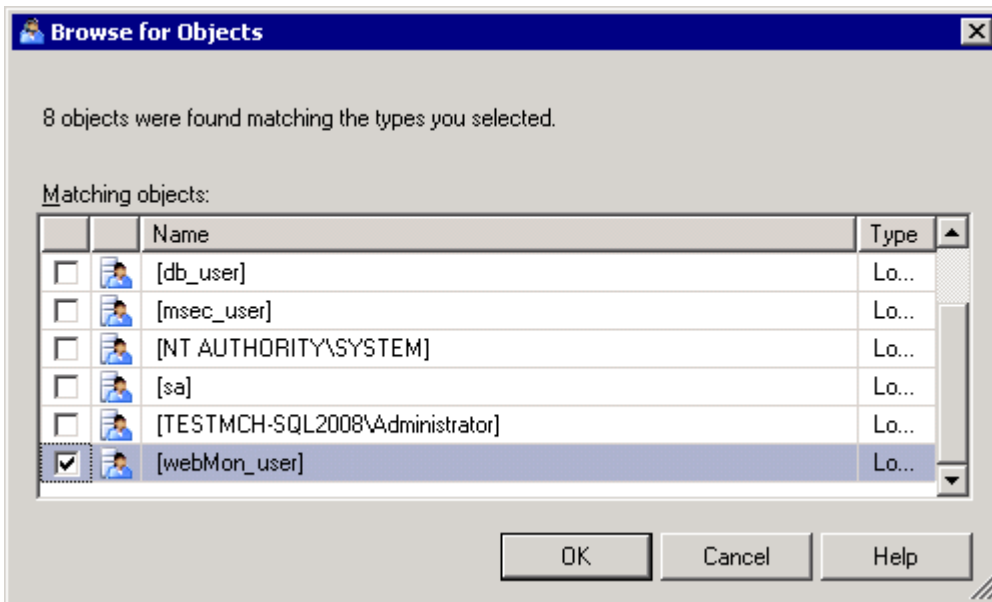
Creating a New Database in Microsoft SQL Server 2008

1. On the SQL server machine, navigate to **Start ► All Programs ► Microsoft SQL Server 2008 ► SQL Server Management Studio**.
2. Key in the database administrator credentials.
3. From the left panel expand **SQL Server node ► Security**.



Screenshot 74 - Create new SQL login

4. Right-click **Logins** and select **New Login**.
5. Key in a valid user login name (example webMon_user).
6. Select the authentication type and click **OK** to apply changes.
7. From the left panel right-click **Databases** folder and select **New Database**.
8. In the new database dialog, key in a valid name (for example WEBMONDB).
9. Click the Owner browse (...) button to select the user created earlier from the **Select Database Owner** dialog.
10. Click **Browse**.



Screenshot 75 - Browse for Objects dialog

11. Select the user created earlier and click **OK**.
12. Click **OK** to close the **Select Database Owner** dialog and **OK** in the **New Database** dialog to apply changes.



To view more information on how to create a new database on various Microsoft SQL Server versions, refer to KBase article:
<http://kbase.gfi.com/showarticle.asp?id=KBID003379>

7.6.2 Enabling Reporting

To enable information gathering for reporting purposes:

1. Navigate to **Configuration ► Reporting**.

Reporting Save Settings Cancel

Reporting records statistical information to a database. You can then use the GFI WebMonitor ReportPack to generate reports of your choice based on the data collected. This dialog allows you to configure the database backend for the reports.

Enable Reporting

SQL Server Reporting

SQL Server:
SQLSRVWEBM

User:
WebMon_user

Password:
●●●●●●●●

Database:
WEBM Get Database List

Back Track Data

Status: 408 records are available starting from 1/24/2011

GFI WebMonitor automatically transfers all live data logged during the day directly to the Microsoft SQL Server backend database you configured above when reporting is enabled.

If reporting has been disabled, GFI WebMonitor will keep track of all of the data which has not yet been transferred to the Microsoft SQL Server backend database.

Back Track allows you to retrieve all of this data and save it to the Microsoft SQL Server backend database.

Back Track Data Now

Screenshot 76 - Configuration: Reporting view

2. Check the **Enable Reporting** checkbox to enable reporting feature.
3. Key in the **SQL Server**, the **User/Password** combination and the **Database** name that enables GFI WebMonitor to connect and audit data to the database in the respective order.



To retrieve the list of available databases, click the **Get Database List** button.

4. Click **Save Settings**.



For security purposes, passwords can only be keyed in from the machine where GFI WebMonitor is installed. Thus, users who are allowed Administrative Access Control from their machine will not be able to view the list of available databases.

7.6.3 Disabling Reporting

To disable information gathering for reporting purposes:

1. Navigate to **Configuration ► Reporting**.
2. Uncheck the **Enable Reporting** checkbox to disable reporting feature.
3. Click **Save Settings**.

7.6.4 Updating Reporting Data

Daily at midnight, GFI WebMonitor automatically transfers any logged data to the Microsoft SQL Server backend database (the same database configured when enabling the reporting feature). There are instances however when the data retrieval process needs to be triggered manually, such as:

- » When upgrading the version of GFI WebMonitor
- » When migrating data stored in files in a storage location to a central database
- » To test configuration settings.

In these cases and others, click the **Update Reporting Data Now** button to trigger the transfer process.



Data is always collected for complete 24-hour periods from midnight to midnight. Thus, the **Update Reporting Data Now** feature does not collect data for partial periods, example between midnight and the time when this button is clicked.

7.7 Safe Search

Safe Search is a feature supported by a number of search engines. If enabled, GFI WebMonitor enforces filtering of explicit email and images from user searches.

Safe Search is compatible with the following search engines:

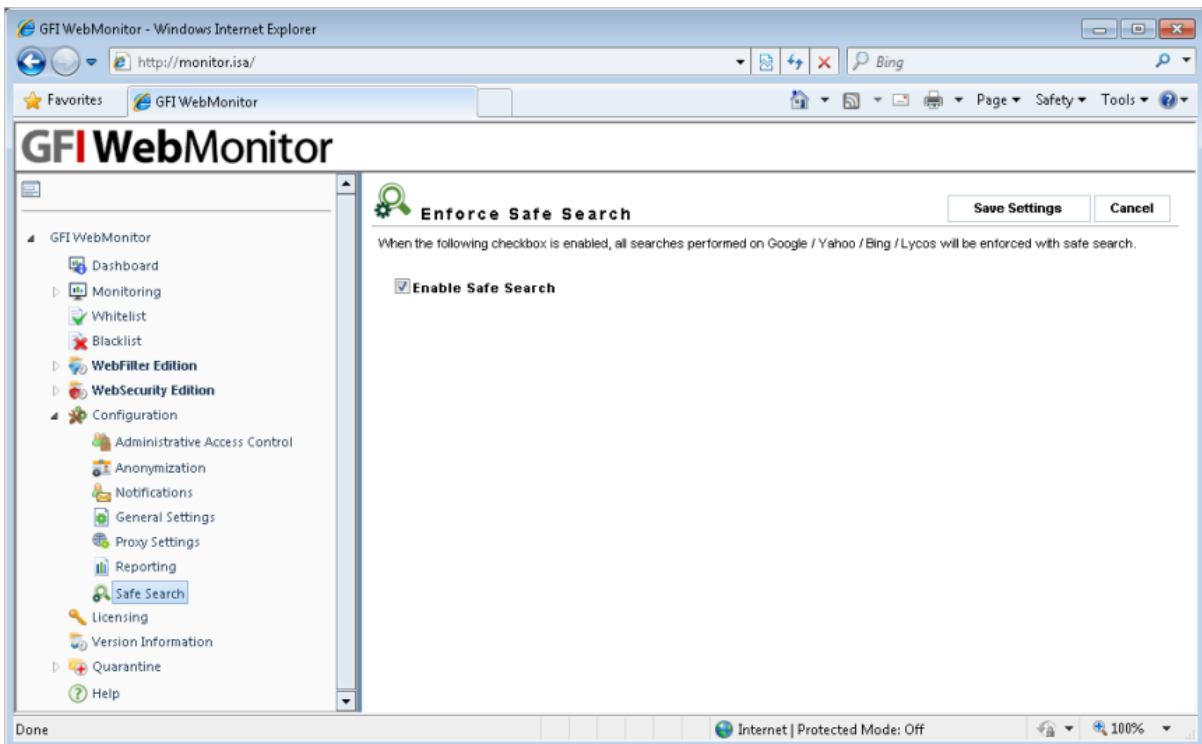
- » Google
- » Yahoo
- » Lycos
- » Bing



The Safe Search feature is available in the **GFI WebMonitor WebFilter Edition**.

7.7.1 Enabling Safe Search

1. Navigate to **Configuration ► Safe Search**.
2. Select **Enable Safe Search**.
3. Click **Save Settings**.



Screenshot 77 - Enabling Safe Search

7.7.2 Disabling Safe Search

1. Navigate to **Configuration ► Safe Search**.
2. Uncheck the **Enable Safe Search** checkbox.
3. Click **Save Settings**

8.1 Introduction

The **Quarantine** node and its sub-nodes enable you to view quarantined items categorized according to the policy they triggered, as well as enable you to either approve or delete the quarantined items. An item can be:

- › an unauthorized site
- › an unauthorized downloaded file, or
- › a virus infected downloaded file.

The following GFI WebMonitor policies can be set to quarantine these items:

- › Web Filtering Policies
- › Download Control Policies
- › Virus Scanning Policies



If Anonymization is enabled, personal data (such as User Names and IPs) will be masked. For more information refer to the [Anonymization](#) section in this manual.

GFI WebMonitor does not store the downloaded files, but it stores their respective URL, same as for the unauthorized sites.

Administrators should review the quarantine to:

- › Establish the reason for which an item is being quarantined
- › Determine whether the item is unauthorized/harmful or not
- › Determine whether the item should be approved or not.

If approved from the quarantine list, items are transferred to the **Temporary Whitelist** and can then be accessed on a temporary basis by the user who triggered the policy.

If deleted from the quarantine list, only the entry is deleted and thus, the items will continue to be quarantined by the respective policies.

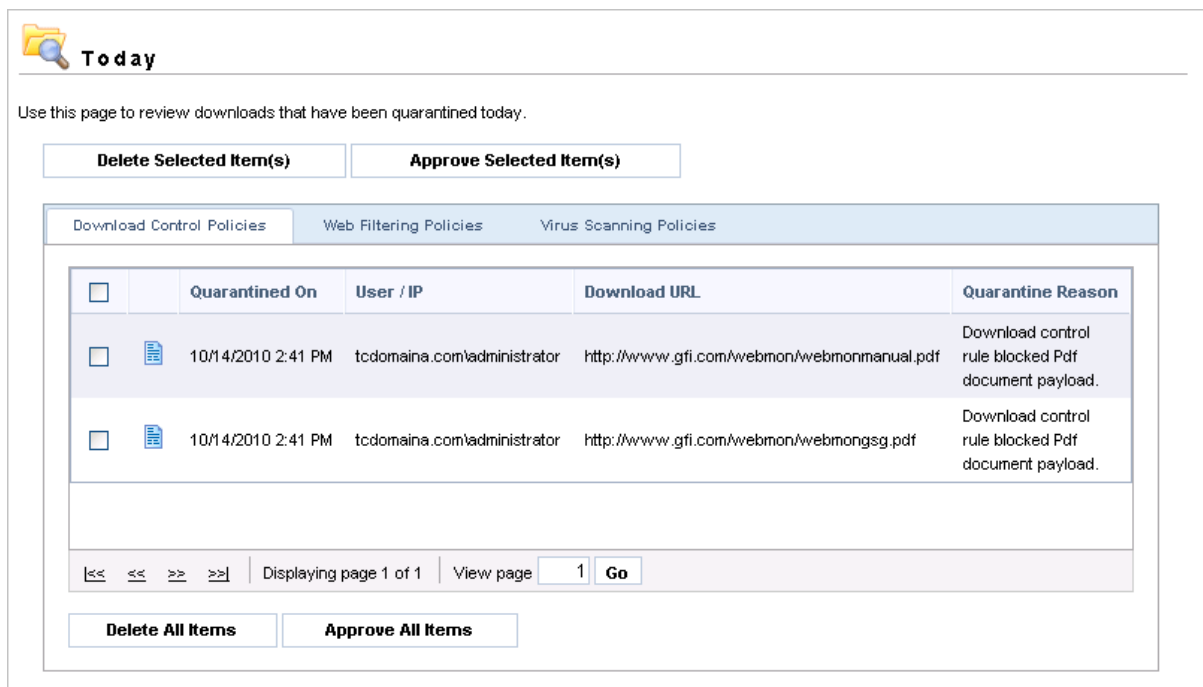
Users can again be forbidden access to the items through the Temporary Whitelist feature. For more information, refer to the [Deleting Items From the Temporary Whitelist](#) section in the **Allowing and blocking users, IP addresses and sites** chapter.

There are four different views for quarantined items:

VIEW	DESCRIPTION
Today	Displays all items transferred to quarantine today
Yesterday	Displays all items transferred to quarantine yesterday
This Week	Displays all items transferred to quarantine on the last 7 days starting from today
All Items	Displays all items currently in quarantine



8.2 Viewing Quarantined Items

The **Today**, **Yesterday**, **This Week** and **All Items** lists display all items quarantined during the specified periods and categorized according to the policy they triggered.



Screenshot 78 - Quarantine view

To view quarantined items:

1. Navigate to the **Quarantine** node, and select one of the views available to view either all the quarantined items or just those for a specified period.
2. Click the required policy tab to view a list of items quarantined for each respective policy category:
 - » **Download Control Policies** tab
 - » **Web Filtering Policies** tab
 - » **Virus Scanning Policies** tab
3. Click the details icon  to view specific details for that item.
4. Click **Go Back To List** to move back to the list of quarantined items.
5. Use the navigation icons  to navigate through long lists of quarantined items.

The information displayed includes:

COLUMN	DESCRIPTION
Quarantined On	The date and time the item was quarantined upon violation of policy
User/IP	The user/IP who violated the policy
Download URL	The URL of the downloaded file or of the unauthorized site
Quarantine Reason	The reason why the item was quarantined

Table Sorting

The lists are sorted by **Quarantined On** in descending order.

8.3 Approving Quarantined Items

The **Today**, **Yesterday**, **This Week** and **All Items** lists enable you to approve any of the quarantined items which are then transferred to the Temporary Whitelist. This way users are allowed temporary access to these items.

To approve one or more items in quarantine:


1. Navigate to the **Quarantine** node, and select one of the views available, depending on when the item was quarantined.
2. Click the policy tab where the quarantined items are listed.






Quarantine Item		
Delete Item	Approve Item	Go Back To List
Downloaded By	tcdomaina.com\administrator	
Download URL	http://www.gfi.com/webmon/webmonmanual.pdf	
Quarantine Reason	Download control rule blocked Pdf document payload.	
Quarantined On	10/14/2010 2:41 PM	

Screenshot 79 - Quarantined item details view

3. To make the downloaded files or accessed URLs available to users:

- » **Option 1:** Click the details icon  to view specific details for an item and click the **Approve Item** button.
- » **Option 2:** Select the checkboxes of individual items and click the **Approve Selected Item(s)** button.
- » **Option 3:** Click the **Approve All Items** button.


	For more information, refer to the Allowing and Blocking Users, IP Addresses and Sites chapter in this manual.
	Exert extreme caution with this feature. By approving an item from the Quarantine, you are excluding the website from all policies configured in GFI WebMonitor for that particular user. Approving a potentially harmful file may therefore lead to your network being compromised.
	The user email address is shown only if the user has been authenticated, and has a valid Active Directory email field.

8.4 Deleting Quarantined Items

The **Today**, **Yesterday**, **This Week** and **All Items** lists enable you to delete quarantined items. When deleted, users will not be allowed access to these items and further attempts will still be quarantined by the respective policies.

To delete one or more items in quarantine:

1. Navigate to the **Quarantine** node, and select one of the views available, depending on when the item was quarantined.

2. Click the policy tab where the quarantined items are listed.
3. To delete the items' entries:
 - > **Option 1:** Click the details icon  to view specific details for an item and click the **Delete Item** button.
 - > **Option 2:** Select the checkboxes of individual items and click the **Delete Selected Item(s)** button.
 - > **Option 3:** Click the **Delete All Items** button.

9 Troubleshooting

9.1 Introduction

The troubleshooting chapter explains how you should go about resolving any software issues that you might encounter. The main sources of information available to users are:

- » The manual - most issues can be solved by reading this manual
- » GFI Knowledge Base articles
- » Web forum
- » Contacting GFI Technical Support

9.2 Knowledge Base

GFI maintains a comprehensive Knowledge Base repository, which includes answers to the most common problems. Refer to the Knowledge Base when the information in this manual does not solve any problems that might be encountered. The Knowledge Base contains the most up-to-date listing of technical support questions and patches. Access the Knowledge Base by visiting: <http://kbase.gfi.com/>.

9.3 Web Forum

User to user technical support is available via the web forum. The forum can be found at: <http://forums.gfi.com/>.

9.4 Request Technical Support

If you have referred to this manual and our Knowledge Base articles, and you still cannot solve issues with the software, contact the GFI Technical Support team by filling in an online support request form or by phone.

ACTION	DESCRIPTION
Online	Fill out the support request form on: http://support.gfi.com/supportrequestform.asp . Follow the instructions on this page closely to submit your support request
Phone	To obtain the correct technical support phone number for your region visit http://www.gfi.com/company/contact.htm



Before you contact our Technical Support team, have your Customer ID available. Your Customer ID is the online account number that is assigned to you when you first register your license keys in our Customer Area at <https://customers.gfi.com/login.aspx>.

We will answer your query within 24 hours or less, depending on your time zone.

9.5 Build Notifications

We recommend that you subscribe to our build notifications list. This way, you will be immediately notified about new product builds. To subscribe to our build notifications, visit: <http://www.gfi.com/pages/productmailing.htm>

10 Glossary

TERM	DEFINITION
Access Control	A feature that allows or denies users access to resources, for example, Internet access.
Active Directory	A technology that provides a variety of network services, including LDAP-like directory services.
AD	See Active Directory
Administrator	The person responsible for installing and configuring GFI WebMonitor.
Anti-virus	Software that detects viruses on a computer.
Bandwidth	The maximum amount of data transferred over a medium. Typically measured in bits per second.
Blacklist	A list that contains information about what should be blocked by GFI WebMonitor.
Cache	A location where GFI WebMonitor temporarily stores downloaded files. This will speed up subsequent requests for the same file as GFI WebMonitor would serve the file directly from the cache instead of downloading it again.
CER	See CER file format
CER file format	A certificate file format that contains the certificate data but not the private key.
Certificate Revocation List	A list issued by a Certification Authority listing HTTPS websites' certificates that were revoked.
Chained Proxy	When client machines connect to more than one proxy server before accessing the requested destination.
Console	An interface that provides administration tools that enable the monitoring and management of Internet traffic.
CRL	See Certificate Revocation List
Dashboard	Enables the user to obtain graphical and statistical information related to GFI WebMonitor operations.
Expired Certificate	An expired certificate has an end date that is earlier than the date when the certificate is validated by GFI WebMonitor.
File Transfer Protocol	A protocol used to transfer files between computers.
FTP	See File Transfer Protocol.
Google Chrome	A web browser developed and distributed by Google.
GPO	See Group Policy Objects.
Group Policy Objects	An Active Directory centralized management and configuration system that controls what users can and cannot do on a computer network.
Hidden Downloads	Unwanted downloads from hidden applications (for example, trojans) or forgotten downloads initiated by users.
HTTP	See Hypertext Transfer Protocol.
HTTPS	See Hypertext Transfer Protocol over Secure Socket Layer (SSL).
Hypertext Transfer Protocol	A protocol used to transfer hypertext data between servers and Internet browsers.
Hypertext Transfer Protocol over Secure Socket Layer (SSL)	A protocol used to securely transfer encrypted hypertext data between servers and Internet browsers using certificates. The URL of a secure connection (SSL connection) starts with https:// instead of http://.
Internet Browser	An application installed on a client machine that is used to access the Internet.
Internet Gateway	A computer that has both an internal and an external network card. Internet sharing is enabled, and client machines on the internal network use this computer to access the Internet.

TERM	DEFINITION
LAN	See Local Area Network.
LDAP	See Lightweight Directory Access Protocol.
Lightweight Directory Access Protocol	A set of open protocols for accessing directory information such as email addresses and public keys.
Local Area Network	An internal network that connects machines in a small area.
Malware	Short for malicious software. Unwanted software designed to infect a computer such as a virus or a trojan.
Microsoft Forefront Threat Management Gateway	A Microsoft product that provides firewall and web proxy services. It also enables administrators to manage Internet access through policies. It is the successor of the Microsoft ISA Server and is part of the Microsoft Forefront line of business security software.
Microsoft Forefront TMG	See Microsoft Forefront Threat Management Gateway
Microsoft Internet Explorer	A web browser developed and distributed by Microsoft Corporation.
Microsoft Internet Security and Acceleration Server	A Microsoft product that provides firewall and web proxy services. It also enables administrators to manage Internet access through policies.
Microsoft ISA Server	See Microsoft Internet Security and Acceleration Server.
Microsoft SQL Server	A Microsoft database management system used by GFI WebMonitor to store and retrieve data.
Microsoft Windows Live Messenger	An instant messaging application developed by Microsoft used by users to communicate on the Internet.
Mozilla Firefox	Mozilla Firefox is an open source Internet browser.
MSN	See Microsoft Windows Live Messenger
Non-validated Certificate	A non-validated certificate has a start date that falls after the date when the certificate is validated by GFI WebMonitor.
NT LAN Manager	A Microsoft network authentication protocol.
NTLM	See NT LAN Manager.
Personal Information Exchange file format	A certificate file format that contains the certificate data and its public and private keys.
PFX	See Personal Information Exchange file format.
Phishing	The act of collecting personal data such as credit card and bank account numbers by sending fake emails which then direct users to sites asking for such information.
Port Blocking	The act of blocking or allowing traffic over specific ports through a router.
Proxy Server	A server or software application that receives requests from client machines and responds according to filtering policies configured in GFI WebMonitor.
Quarantine	A temporary storage for unknown data that awaits approval from an administrator.
Revoked Certificate	A revoked certificate is a valid certificate that has been withdrawn before its expiry date (for example, superseded by a newer certificate or, have a lost or exposed private key).
Spyware	Unwanted software that publishes private information to an external source.
Traffic Forwarding	The act of forwarding internal/external network traffic to a specific server through a router.
Uniform Resource Locator	The address of a web page on the world wide web. It contains information about the location and the protocol.
URL	See Uniform Resource Locator.

TERM	DEFINITION
User Agent	A client application that connects to the Internet and performs automatic actions.
Virus	Unwanted software that infects a computer.
WAN	See Wide Area Network.
Web Proxy AutoDiscovery protocol	An Internet protocol used by browsers to automatically retrieve proxy settings from a WPAD data file.
Web traffic	The data sent and received by clients over the network to websites.
WebFilter Edition	A configurable database that allows site access according to specified site categories per user/group/IP address and time.
WebGrade Database	A database in GFI WebMonitor, used to categorize sites.
WebSecurity Edition	WebSecurity contains multiple anti-virus engines to scan web traffic accessed and downloaded by the clients.
Whitelist	A list that contains information about what should be allowed by GFI WebMonitor.
Wide Area Network	An external network that connects machines in large areas.
WPAD	See Web Proxy AutoDiscovery protocol.

Index

A

Access Control 79, 80, 101
Anonymization 15, 22, 81, 95
Anti-virus Scanning Engines 72, 73

B

Blacklist Node 27, 30
Build Notifications 99

C

Chained Proxy 101
Configuring GFI WebMonitor 79

D

Dashboard node 5
Download Control Policy 53, 54, 58

F

File Scanning Cache 85, 86

H

Hidden downloads 17, 18, 101
HTTP 2, 10, 101
HTTPS Scanning 87

I

IM Control Policy 60, 63, 64
Internet Gateway 101

L

LDAP 101
License key 99

M

Malware 102
Microsoft Forefront TMG 1, 102
Microsoft ISA Server 1, 102

Monitoring node 11, 22, 87
MSN 53, 60, 61, 102

O

Online lookups 50, 51

P

Phishing 12, 53, 76, 77, 78, 102
Port Blocking 102
Proxy Server 85, 101

Q

Quarantine Node 11, 96, 98

R

Reporting Node 88

S

Safe Search 92, 93
Spyware 53, 72, 74

T

Technical Support 99
Temporary Whitelist Area 86
Traffic Forwarding 102

U

User Agent 17, 18, 103

W

Web Forum 99
Web traffic 1, 103
WebFilter Edition Node 33
WebGrade Database 50, 51, 83, 103
WebSecurity Edition Node 53
Whitelist Node 28
Wildcards 29, 30, 31
WPAD 103

USA, CANADA AND CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104, Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

Email: ussales@gfi.com

UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

Email: sales@gfi.co.uk

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

Email: sales@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

Email: sales@gfiap.com



Disclaimer

© 2011. GFI Software. All rights reserved. All product and company names herein may be trademarks of their respective owners. The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.
