
GFI WebMonitor 2009

Administration and Configuration Manual

By GFI Software Ltd.



<http://www.gfi.com>
E-mail: info@gfi.com

Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of GFI SOFTWARE LTD.

Last updated: May 28, 2010

Version number: WEBMON-ACM-EN-2.0.0

Contents

1	Introduction	1
1.1	About this manual	1
1.2	Terms used in this manual	1
2	Using the GFI WebMonitor dashboard	3
2.1	Introduction	3
2.2	The GFI WebMonitor dashboard	3
3	Monitoring Internet activity	9
3.1	Introduction	9
3.2	Active Connections	9
3.3	Past Connections	10
3.4	Hidden Downloads	10
3.4.1	Add hidden downloads to Whitelist	12
3.5	Search	12
3.6	Bandwidth Consumption	14
3.6.1	Top Sites	14
3.6.2	Top Users	15
3.6.3	Top Categories	16
3.7	Sites History	17
3.7.1	Top Time Consumption	17
3.7.2	Top Hits Count	17
3.8	Users History	18
3.8.1	Top Surfers	18
3.8.2	Top Hits Count	19
3.8.3	Top Policy Breakers	20
3.9	Site Access History	21
3.10	User History Details	22
3.11	Activity Log	23
3.12	Viewing data by date	24
3.13	Charts	24
4	Allowing and blocking users, IP addresses and sites	27
4.1	Introduction	27
4.2	Whitelist	27
4.2.1	Preconfigured items	27
4.2.2	Adding items to the Permanent Whitelist	28
4.2.3	Deleting items from the Permanent Whitelist	28
4.2.4	Adding items to the Temporary Whitelist	29
4.2.5	Deleting items from the Temporary Whitelist	30
4.3	Blacklist	30
4.3.1	Adding items to the Blacklist	30
4.3.2	Deleting items from the Blacklist	31
4.4	Using wildcards	31
5	WebFilter Edition - Site rating and content filtering	33
5.1	Introduction	33
5.2	Web Filtering Policies	33

5.2.1	Adding a Web Filtering Policy	34
5.2.2	Editing a Web Filtering Policy	38
5.2.3	Enabling/disabling a Web Filtering Policy	38
5.2.4	Deleting a Web Filtering Policy	38
5.2.5	Default Web Filtering Policy	38
5.3	Configuring advanced Web Filtering Policy conditions	39
5.3.1	Adding an advanced Web Filtering Policy condition	39
5.3.2	Editing an advanced Web Filtering Policy condition	40
5.3.3	Deleting an advanced Web Filtering Policy condition	40
5.4	WebGrade Database	40
5.4.1	Enabling/disabling the WebGrade Database	41
5.4.2	Enabling/disabling online lookups for URLs	41
5.4.3	Configuring WebGrade Database Updates	42
5.4.4	Checking URL Categories	42
6	WebSecurity Edition - File scanning and download control	43
6.1	Introduction	43
6.2	Download Control Policies	43
6.2.1	Adding a Download Control Policy	43
6.2.2	Editing a Download Control Policy	46
6.2.3	Enabling/disabling a Download Control Policy	47
6.2.4	Deleting a Download Control Policy	47
6.2.5	Default Download Control Policy	47
6.2.6	Adding New Content-types	47
6.3	IM (Instant Messaging) Control Policies	48
6.3.1	Adding an IM Control Policy	48
6.3.2	Editing an IM Control Policy	51
6.3.3	Enabling/Disabling an IM Control Policy	52
6.3.4	Deleting an IM Control Policy	52
6.3.5	Default IM Control Policy	52
6.4	Virus Scanning Policies	52
6.4.1	Adding a Virus Scanning Policy	53
6.4.2	Editing a Virus Scanning Policy	56
6.4.3	Enabling/disabling a Virus Scanning Policy	56
6.4.4	Deleting a Virus Scanning Policy	56
6.4.5	Default Virus Scanning Policy	56
6.4.6	Adding New Content-types	57
6.5	Virus & Spyware Protection	57
6.5.1	Enabling/disabling the scanning engines	58
6.5.2	Configuring Anti-Virus Updates	58
6.6	Anti-Phishing Engine	60
6.6.1	Enabling/disabling the Anti-Phishing Engine	60
6.6.2	Configuring Anti-Phishing database updates	61
6.6.3	Configuring phishing notifications	62
7	Configuring GFI WebMonitor	63
7.1	Introduction	63
7.2	Administrative Access Control	63
7.2.1	Adding Users/IP addresses to the access permissions list	63
7.2.2	Deleting Users/IP addresses from the access permissions list	64
7.3	Notifications	64
7.3.1	Configuring the sender of administrative notifications	64
7.3.2	Configuring the recipients of administrative notifications	65
7.3.3	Deleting email recipients	65
7.4	General Settings	65
7.5	Proxy Settings	67
7.5.1	Configuring Network Configuration	68

7.5.2	Configuring Authentication Method	69
7.5.3	Configuring Chained Proxy	71
7.6	Reporting	71
7.6.1	Reporting requirements	72
7.6.2	Enable Reporting	73
7.6.3	Disabling Reporting	74
7.6.4	Updating Reporting Data	75
8	Quarantine	77
8.1	Introduction	77
8.2	Viewing quarantined items	77
8.3	Approving quarantined items	79
8.4	Deleting quarantined items	79
9	Miscellaneous	81
9.1	Introduction	81
9.2	Configuring Network Access policy	81
10	Troubleshooting	87
10.1	Introduction	87
10.2	Common Issues	87
10.3	Knowledge Base	88
10.4	Web Forum	88
10.5	Request technical support	89
10.6	Build notifications	89
11	Glossary	91
	Index	95

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 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 1	Introduces this manual and its use.
Chapter 2	How to access and use GFI WebMonitor's dashboard.
Chapter 3	How to monitor Internet activity.
Chapter 4	How to configure allowed and blocked entities.
Chapter 5	How to configure WebFilter Edition policies.
Chapter 6	How to configure WebSecurity Edition policies.
Chapter 7	How to configure GFI WebMonitor settings.
Chapter 8	How to configure and manage quarantined items.
Chapter 9	Provides information on topics that do not strictly fall within other chapters.
Chapter 10	Provides troubleshooting information on common issues.
Glossary	Explains specific technical terms used in this manual.

Getting Started Guide

Detailed installation guidelines are provided in the **Getting Started Guide**, which is downloadable from the GFI website:

<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.

1.2 Terms used in this manual

The following terms are used in this manual:

“NOTE:”

- Provides additional information and references essential for the operation of GFI WebMonitor.

“IMPORTANT:”

- Provides important information such as warnings and cautions regarding potential issues commonly encountered.

For any technical terms and their definitions as used in this manual, refer to the [Glossary](#) chapter in this manual.

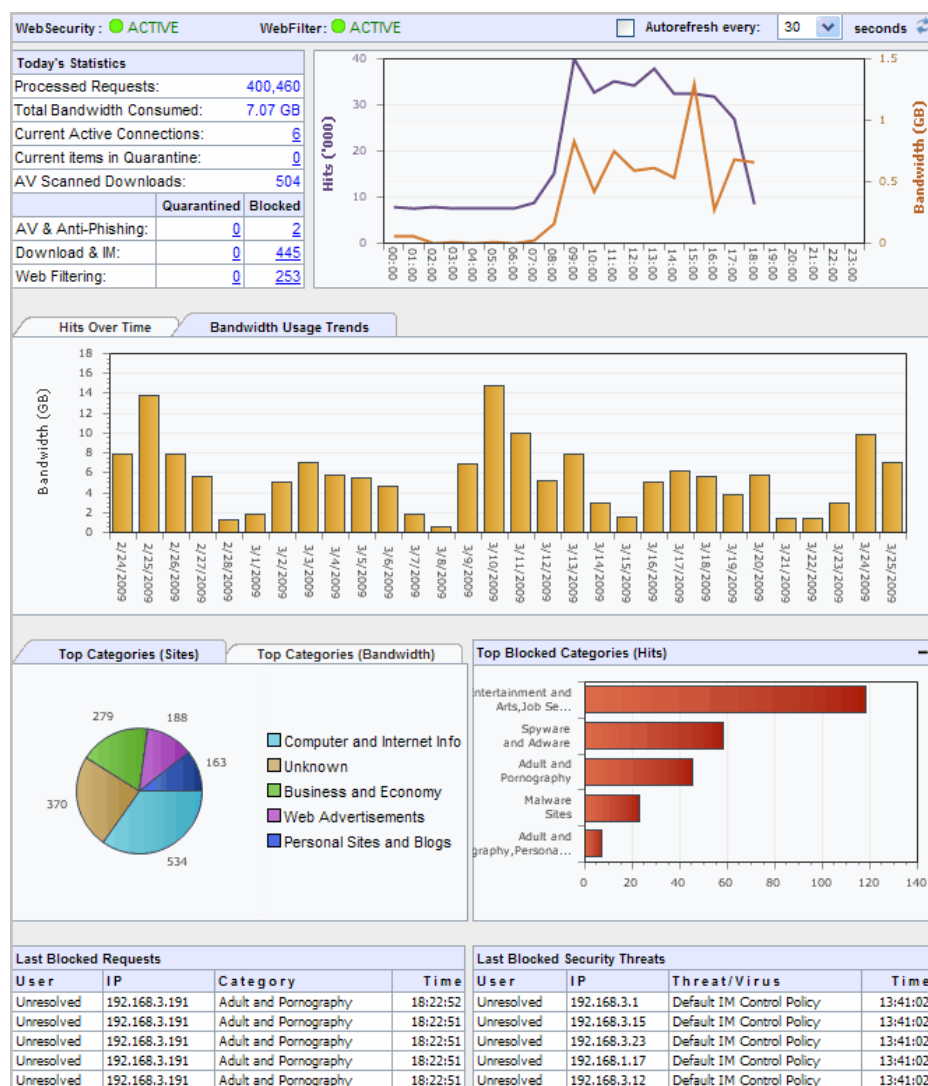
2 Using the GFI WebMonitor dashboard

2.1 Introduction

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

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


2.2 The GFI WebMonitor dashboard



Screenshot 1 - Dashboard view

The **Dashboard** node in the navigation bar allows you to access the GFI WebMonitor Dashboard. The dashboard shows the information described in the sections below.

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

NOTE: Click the refresh button  at the upper right corner to refresh the displayed information.

Statistics

Today's Statistics		
Processed Requests:	1,657	
Total Bandwidth Consumed:	57.31 MB	
Current Active Connections:	0	
Current items in Quarantine:	2	
AV Scanned Downloads:	4	
	Quarantined	Blocked
AV & Anti-Phishing:	0	0
Download & IM:	6	26
Web Filtering:	0	0

Screenshot 2 - Dashboard: Statistics

The information provided in this table lists a number of important operational elements of GFI WebMonitor for the current day (from midnight to the instant the dashboard is launched).

Select the hyperlink next to **Current Active Connections** to view the **Active Connections**, which are also accessible from the **Monitoring** node. For more information, refer to the [Active Connections](#) section in the [Monitoring Internet activity](#) chapter.

Select the hyperlink next to **Current items in Quarantine** to view a summary of the quarantine folder. Quarantined items can also be accessed from the **Quarantine** node. For more information, refer to the [Viewing quarantined items](#) section in the [Quarantine](#) chapter.

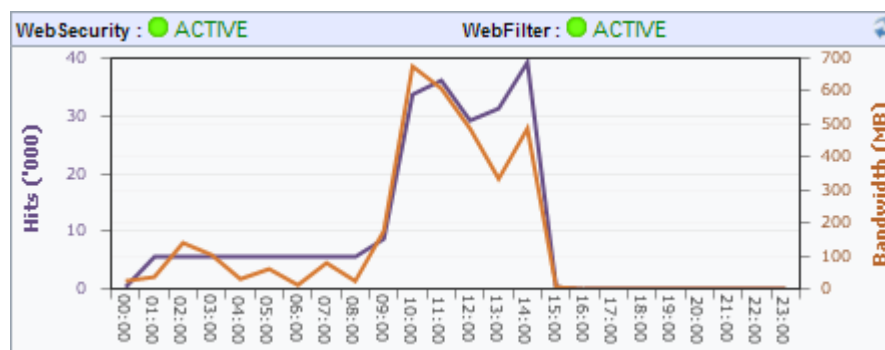
AV Scanned Downloads represents the total downloads scanned by the anti-virus engines. For more information, refer to the section [Virus & Spyware Protection](#) in the [WebSecurity Edition - File scanning and download control](#) chapter.

Select the other hyperlinks within the **Quarantined** and **Blocked** section to view further detail on the statistics as summarized below.

Feature	Quarantined	Blocked
AV & Anti-Phishing	Selecting the hyperlink under Quarantined allows you to approve or delete quarantined items in the Virus Scanning Policies category. For more information, refer to the Viewing quarantined items section in the Quarantine chapter.	Selecting the hyperlink under Blocked allows you to view the Top Policy Breakers Report . For more information, refer to the Top Policy Breakers section in the Monitoring Internet activity chapter.

<p>Download & IM</p>	<p>Selecting the hyperlink under Quarantined allows you to approve or delete quarantined items in the Download Control Policies category.</p> <p>For more information, refer to the Viewing quarantined items section in the Quarantine chapter.</p>	<p>Selecting the hyperlink under Blocked allows you to view the Top Policy Breakers Report.</p> <p>For more information, refer to the Top Policy Breakers section in the Monitoring Internet activity chapter.</p>
<p>Web Filtering</p>	<p>Selecting the hyperlink under Quarantined allows you to approve or delete quarantined items in the Web Filtering Policies category.</p> <p>For more information, refer to the Viewing quarantined items section in the Quarantine chapter.</p>	<p>Selecting the hyperlink under Blocked allows you to view the Top Policy Breakers Report.</p> <p>For more information, refer to the Top Policy Breakers section in the Monitoring Internet activity chapter.</p>

WebSecurity/WebFilter status and usage chart

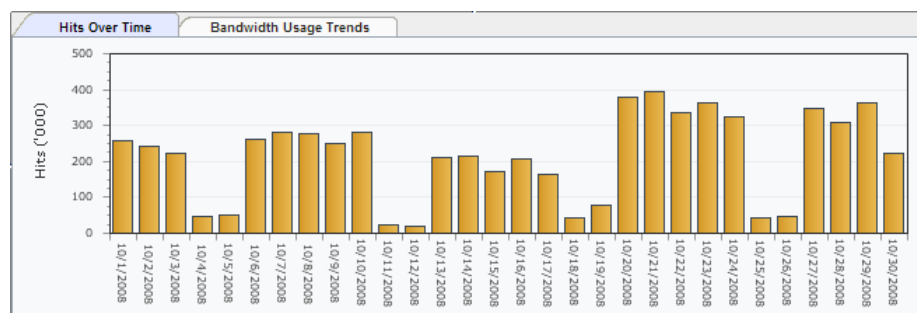


Screenshot 3 - Dashboard: WebSecurity and WebFilter status and usage chart

The **WebSecurity/WebFilter status and usage chart** enables you to:

- Know whether the WebSecurity and WebFilter components are active or not.
- View a graphical representation of the correlation between the number of hits and bandwidth use for the current day (from midnight to the instant the dashboard is launched).

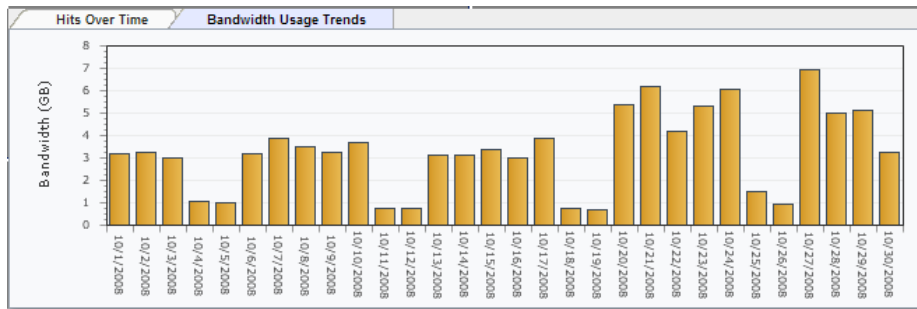
Hits Over Time chart



Screenshot 4 - 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 and includes the current day (from midnight to the instant the dashboard is launched). This enables you to identify a pattern of how website hits fluctuate on a day-by-day basis and to identify any anomalies.

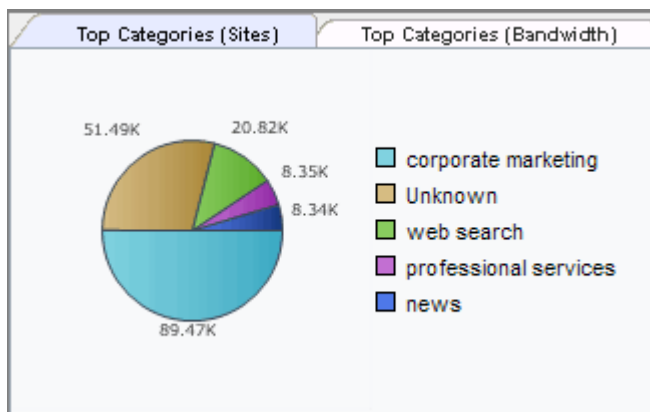
Bandwidth Usage Trends chart



Screenshot 5 - 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 (from midnight to the instant the dashboard is launched). 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.

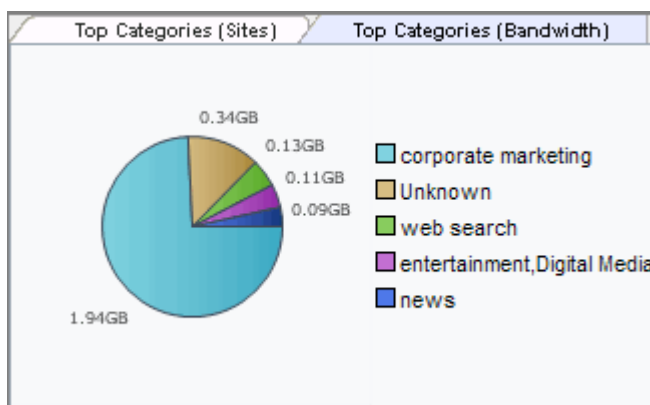
Top Categories (Sites) chart



Screenshot 6 - 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 (from midnight to the instant the dashboard is launched). This enables you to gain knowledge on which categories of sites are being visited by web users.

Top Categories (Bandwidth) chart

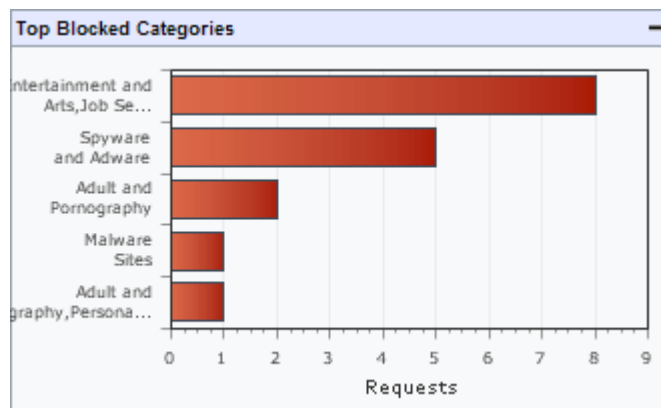


Screenshot 7 - Dashboard: Top Categories (Bandwidth) chart

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

midnight to the instant the dashboard is launched). This enables you to identify how your bandwidth is being utilized vis-à-vis the website categories browsed by users.

Top Blocked Categories (Hits) chart



Screenshot 8 - 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 (from midnight to the instant the dashboard is launched). This enables you to identify the main reasons of why requests were blocked.

Last Blocked Requests list

Last Blocked Requests			
User	IP	Category	Time
Domain\User1	192.168.1.13	consumer shopping	14:04:13
Domain\User1	192.168.1.13	consumer shopping	14:04:13
Domain\User2	192.168.0.30	Digital Media, Radio Stations, Music	14:00:41
Unresolved	192.168.3.191	consumer shopping	13:44:56
Unresolved	192.168.3.191	consumer shopping	13:44:51

Screenshot 9 - Dashboard: Last Blocked Requests list

The **Last Blocked Requests list** displays the most recent five entries for the current day (from midnight to the instant the dashboard is launched) of users/IP addresses whose requests were blocked. 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 list

Last Blocked Security Threats			
User	IP	Threat/Virus	Time
Unresolved	192.168.3.10	Scanned with Bitdefender Scanned with Norman Kaspersky: File could not be scanned. Password protected.	11:54:17
Unresolved	192.168.1.101	Bitdefender: Infected:EICAR-Test-File (not a virus) Norman: Infected with EICAR_Test_file_not_a_virus! Kaspersky: Infected:EICAR-Test-File	10:08:33

Screenshot 10 - Dashboard: Last Blocked Security Threats list

The **Last Blocked Security Threats list** displays the most recent five entries for the current day (from midnight to the instant the dashboard is launched) of users/IP addresses from whose machines GFI WebMonitor detected the threats/viruses. This enables you to identify security issues as early as possible, in time to take preventive measures before your network security is breached.

3 Monitoring Internet activity

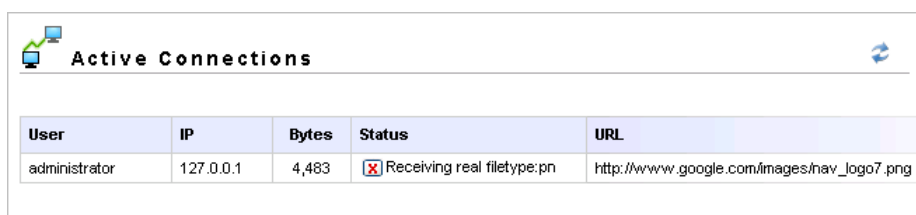
3.1 Introduction

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
- Search
- Bandwidth Consumption
- Sites History
- Users History
- Activity Log

3.2 Active Connections

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



User	IP	Bytes	Status	URL
administrator	127.0.0.1	4,483	[X] Receiving real filetype:pn	http://www.google.com/images/hav_logo7.png


Screenshot 11 - Monitoring: Active Connections view

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

The information displayed includes:

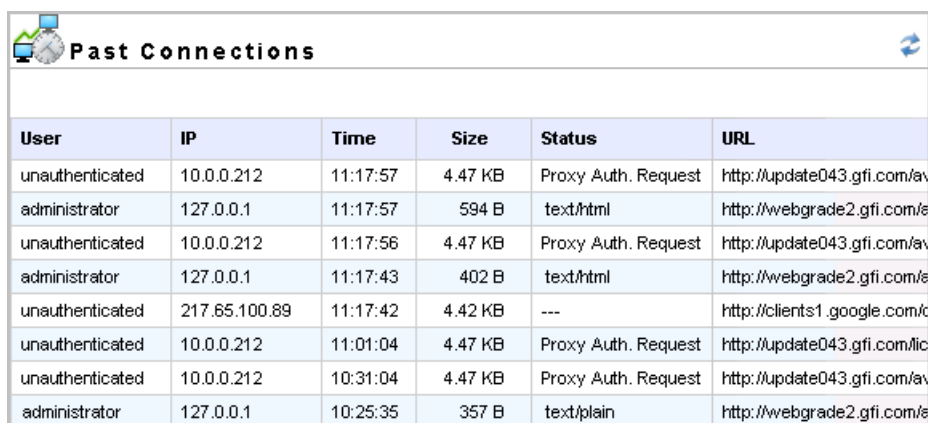
- **User** - the user that is being monitored and whose request is being processed at the instant the report is launched or refreshed
- **IP** - the IP that is being monitored and whose request is being processed at the instant the report is launched or refreshed
- **Bytes** - the size of the download at the instant the report is launched or refreshed
- **Status** - the status of the connection (e.g. 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 (e.g. 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	10.0.0.212	11:17:57	4.47 KB	Proxy Auth. Request	http://update043.gfi.com/av
administrator	127.0.0.1	11:17:57	594 B	text/html	http://webgrade2.gfi.com/e
unauthenticated	10.0.0.212	11:17:56	4.47 KB	Proxy Auth. Request	http://update043.gfi.com/av
administrator	127.0.0.1	11:17:43	402 B	text/html	http://webgrade2.gfi.com/e
unauthenticated	217.65.100.89	11:17:42	4.42 KB	---	http://clients1.google.com/c
unauthenticated	10.0.0.212	11:01:04	4.47 KB	Proxy Auth. Request	http://update043.gfi.com/lic
unauthenticated	10.0.0.212	10:31:04	4.47 KB	Proxy Auth. Request	http://update043.gfi.com/av
administrator	127.0.0.1	10:25:35	357 B	text/plain	http://webgrade2.gfi.com/e

Screenshot 12 - Monitoring: Past Connections view

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

The information displayed includes:

- **User** - the user that is being monitored and whose request was processed
- **IP** - the IP that is 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 (e.g. the file type, the error code, redirection or not modified) that was processed
- **URL** - the URL of the request that was processed

Table Sorting

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

3.4 Hidden Downloads

The **Hidden Downloads** report allows 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.

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 15min after download. Such downloads are also from valid applications (automatic updates etc.). For those, if trusted, its advised to move their download URL domain locations to the [white list](#).

Group By: URL User Agent IP
 Display: All Only Executables and Packages
 View data for: Today

Last Time	Count	Real Filetype	Content Type	URL															
2009-06-15 09:46:23	1	Unknown Attachment	image/x-icon	http://download.typepad.com															
2009-06-15 09:38:28	2	Unknown Attachment	application/json	http://www.lmodules.com/opensocial/makeRequest															
<table border="1"> <thead> <tr> <th>Time</th> <th>User</th> <th>IP</th> <th>Size</th> <th>User Agent</th> </tr> </thead> <tbody> <tr> <td>2009-06-15 09:38:28</td> <td>MYCOMPANY\john</td> <td>192.168.1.3</td> <td>2.1 KB</td> <td>Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.9.0.10)</td> </tr> <tr> <td>2009-06-15 09:38:28</td> <td>MYCOMPANY\john</td> <td>192.168.1.3</td> <td>0 B</td> <td>Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.9.0.10)</td> </tr> </tbody> </table>					Time	User	IP	Size	User Agent	2009-06-15 09:38:28	MYCOMPANY\john	192.168.1.3	2.1 KB	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.9.0.10)	2009-06-15 09:38:28	MYCOMPANY\john	192.168.1.3	0 B	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.9.0.10)
Time	User	IP	Size	User Agent															
2009-06-15 09:38:28	MYCOMPANY\john	192.168.1.3	2.1 KB	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.9.0.10)															
2009-06-15 09:38:28	MYCOMPANY\john	192.168.1.3	0 B	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.9.0.10)															
2009-06-15 09:36:35	1	Unknown Attachment	application/json	http://fka9ybe9u4sq98ip8rfv007atcn3d.iq.qmodules.com/gadgets/makeRe															
2009-06-15 09:27:00	1	Executable	application/octet-stream	http://downloadfree.asa.com/update/u7avi2176u21452.bin															
2009-06-15 09:26:53	1	Executable	application/octet-stream	http://downloadfree.aton.com/update/u7avi1564u1495ht.bin															
2009-06-15 09:18:17	1	Executable	application/octet-stream	http://dl.google.com/picasa/public-update-7143.exe															

Screenshot 13 - Monitoring: Hidden Downloads view

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

The information displayed includes:

- **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:

- **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:

- **URL** to show the URL of the downloaded file.
- **User Agent** to display the agent that started the hidden download.
- **IP** to display the IP address of the URL that started the hidden download.

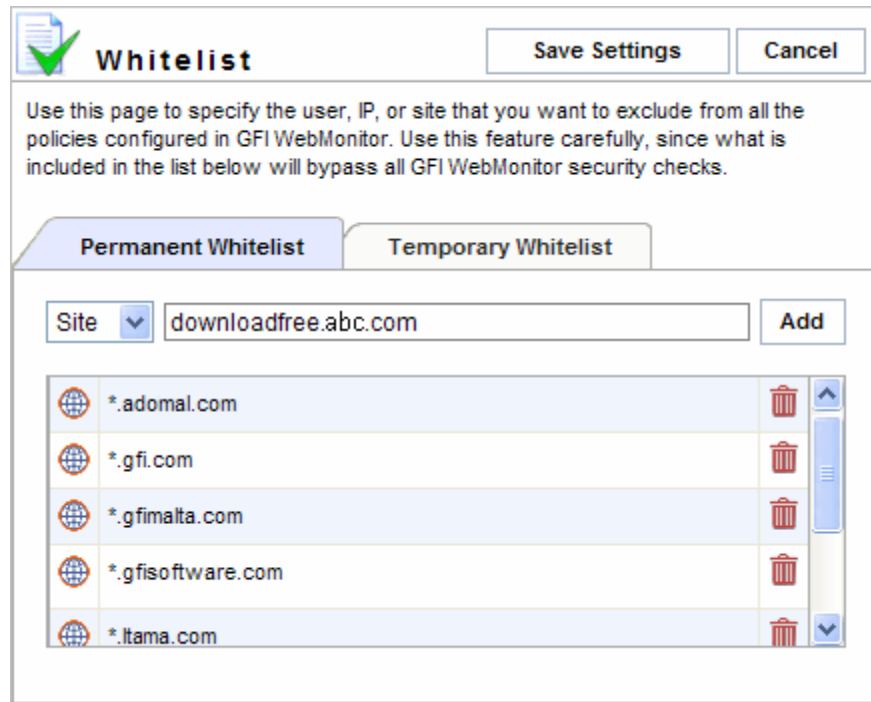
From the **Display** radio buttons select one of the following options:

- **All** to display entries for all file types.
- **Only Executables and Packages** to display 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



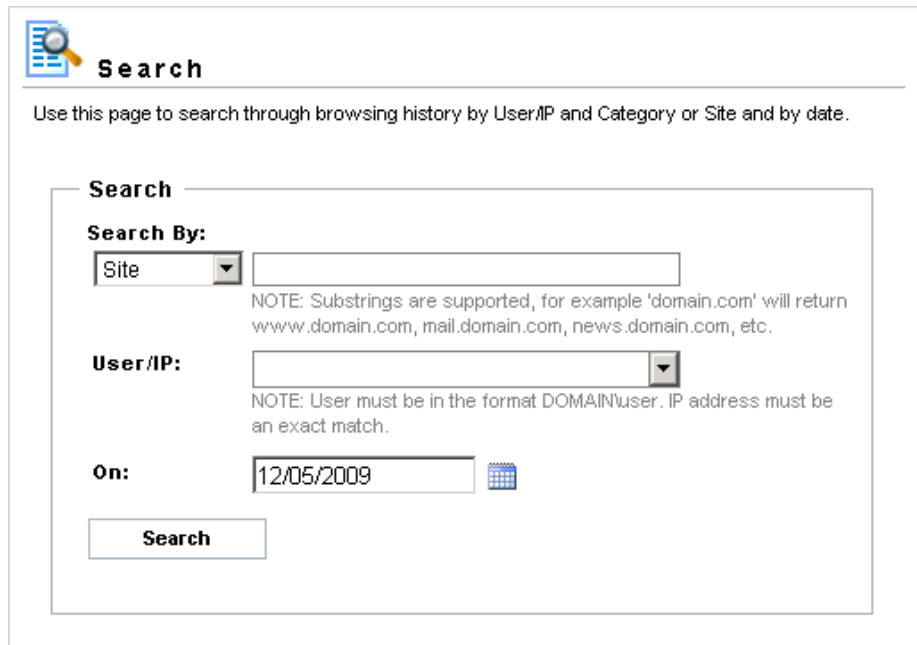
Screenshot 14 - Whitelist hidden downloads dialog

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 through the browsing history for a specific date for:

- a specific site or domain, or a specific category, or
- a specific user, or
- a combination of both, or
- all categories and all users.



Search

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

Search


Search By:

Site

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

User/IP:

NOTE: User must be in the format DOMAIN\user. IP address must be an exact match.

On: 

Search

Screenshot 15 - Monitoring: Search view

To search an item:

1. Navigate to **Monitoring ► Search** to access the **Search** view.
2. From the **Search By** drop-down list, key in the **Site** or select the **Category** required.
3. From the **User/IP** drop-down list, key in or select the User or IP address.

NOTE: When keying in a **User** in the related search text box, specify the username in the format DOMAIN\user.

4. Specify the date required and click **Search** to open the **Search Results for...** view.

The information displayed within the **Search Results for...** view depends on the search criteria specified:

Site only	Displays all the websites belonging to the specified URL or domain, visited by all users on the specified date.
Category only	Displays all the websites belonging to the specified category, visited by all users on the specified date.
User only	Displays all the websites, visited by the specified user on the specified date.
Site and User	Displays all the websites belonging to the specified URL or domain, visited by the specified user on the specified date.
Category and User	Displays all the websites belonging the specified category, visited by the specified user on the specified date.
All Categories and Any User	Displays all the categories visited by all users on the specified date.

Depending on the search criteria specified, the information displayed includes:

- **Show Traffic Over Time Chart** - for more information, refer to the [Charts](#) section in this chapter.
- **Show Hits Over Time Chart** - for more information, refer to the [Charts](#) section in this chapter.
- **Show IM Messages Over Time Chart** - for more information, refer to the [Charts](#) section in this chapter.

- **Bandwidth (DL/UL)** - the total bandwidth used by each site or by each web category
- **File Types** - the types of files accessed from each site followed by the number of times each file type was accessed in brackets
- **Hits** - the total number of requests (more than one request can be submitted for the same site) by the user.
- **Number of Sites** - the number of sites that were accessed by the users, which form part of the category
- **Number of Users** - the number of users that accessed the sites which form part of the category
- **Site** - the site that was accessed by the user
- **Usage (DL/UL)** - the total bandwidth used by each user
- **User/IP** - the user/IP that is being monitored
- **Web Category** - the classification of which the accessed site forms part of

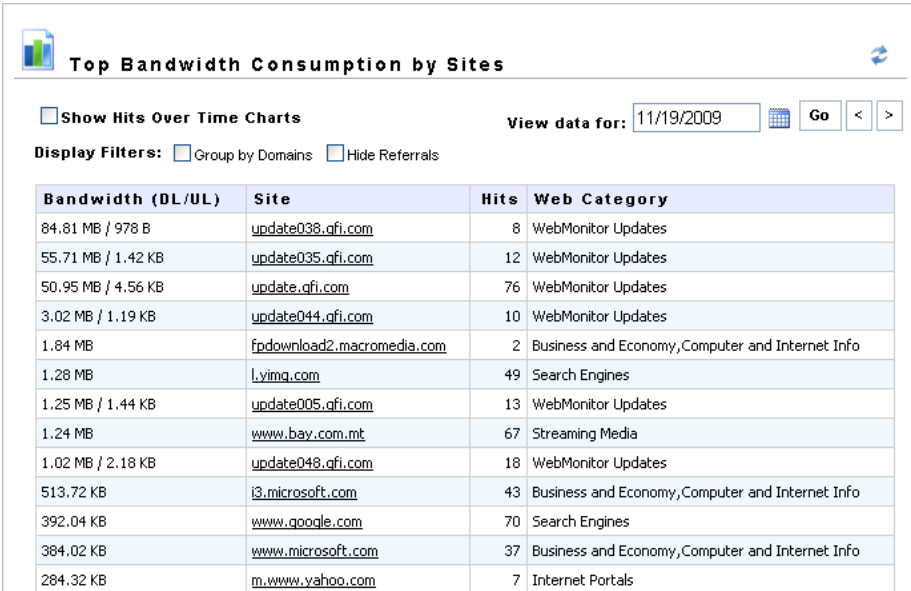
3.6 Bandwidth Consumption

The **Bandwidth Consumption** reports allows you to monitor bandwidth usage. Three types of reports are available:

- Top Sites
- Top Users
- Top Categories

3.6.1 Top Sites

The **Top Sites** report displays the amount of bandwidth consumed by visited websites on a specific date.



Bandwidth (DL/UL)	Site	Hits	Web Category
84.81 MB / 978 B	update038.qfi.com	8	WebMonitor Updates
55.71 MB / 1.42 KB	update035.qfi.com	12	WebMonitor Updates
50.95 MB / 4.56 KB	update.qfi.com	76	WebMonitor Updates
3.02 MB / 1.19 KB	update044.qfi.com	10	WebMonitor Updates
1.84 MB	fpdownload2.macromedia.com	2	Business and Economy, Computer and Internet Info
1.28 MB	l.vimq.com	49	Search Engines
1.25 MB / 1.44 KB	update005.qfi.com	13	WebMonitor Updates
1.24 MB	www.bay.com.mt	67	Streaming Media
1.02 MB / 2.18 KB	update048.qfi.com	18	WebMonitor Updates
513.72 KB	i3.microsoft.com	43	Business and Economy, Computer and Internet Info
392.04 KB	www.google.com	70	Search Engines
384.02 KB	www.microsoft.com	37	Business and Economy, Computer and Internet Info
284.32 KB	m.www.yahoo.com	7	Internet Portals

Screenshot 16 - Bandwidth Consumption: Top Sites report

Navigate to **Monitoring ► Bandwidth Consumption ► Top Sites** to access the **Top Sites** report.

The information displayed includes:

- **Show Hits Over Time Chart** - for more information, refer to the [Charts](#) section in this chapter.

- **Group by Domains** - (in the Display Filters group) when selected the list is grouped by website-visited domain.
- **Hide Referrals** - (in the Display Filters group) when selected the list displays only the URLs of the sites which most likely were entered manually by the user.
- **Bandwidth (DL/UL)** - the total bandwidth used by each site
- **Site** - the site that was accessed by the users
- **Hits** - the total number of requests (more than one request can be submitted for the same site) by the user
- **Web Category** - the classification of which the accessed site forms part of

Table Sorting

By default, the lists are sorted by **Bandwidth** in descending order, but all columns can be sorted in either ascending or descending order by clicking on the appropriate column heading.

Further Information

Select the **Site** hyperlink to view the **Site Access History**. For more information, refer to the [Site Access History](#) section in this chapter.

3.6.2 Top Users

The **Top Users** report displays the amount of bandwidth consumed by users/IP addresses on a specific date.

User / IP	Usage (DL/UL)	Hits	Sites Accessed
127.0.0.1	200.92 MB / 61.12 KB	640	64 sites - 207.46.110.49, ads1.msn.com, c.microsoft.com, clients1.google.com, cri.verisign.com, ...
192.168.5.10	3.08 MB / 176 B	352	43 sites - a.ads2.msn.com, a.rad.msn.com, activex.microsoft.com, ad.doubleclick.net, ad.wsod.com, ...

Screenshot 17 - Bandwidth Consumption: Top Users report

Navigate to **Monitoring ► Bandwidth Consumption ► Top Users** to access the **Top Users** report.

The information displayed includes:

- **Show Hits Over Time Chart** - for more information, refer to the [Charts](#) section in this chapter.
- **User/IP** - the user/IP that is being monitored
- **Usage (DL/UL)** - the total bandwidth used by each user
- **Hits** - the total number of requests (more than one request can be submitted for the same site) by the user
- **Sites Accessed** - the total number and names of different sites accessed by the user

Table Sorting

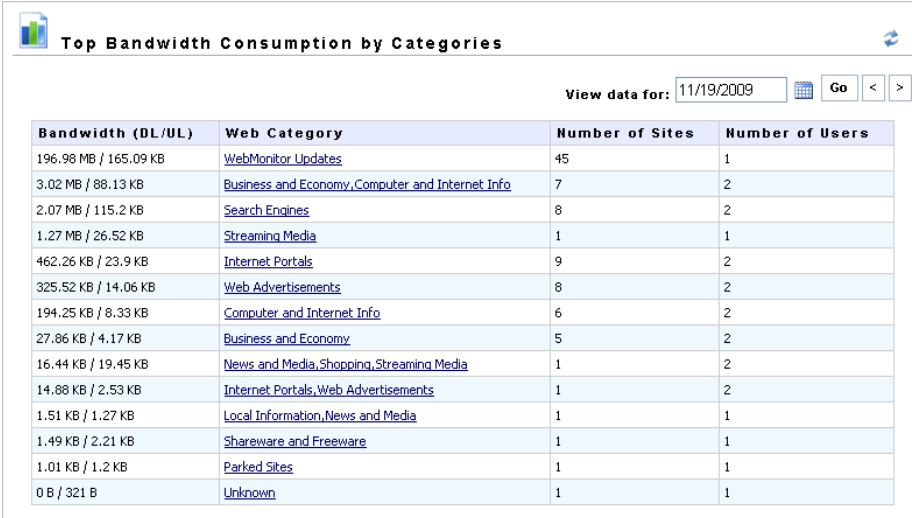
By default, the list is sorted by **Usage (DL/UL)** in descending order, but all columns apart from **Sites Accessed** can be sorted in either ascending or descending order by clicking on the appropriate column heading.

Further Information

Select the **User/IP** hyperlink to view the **User History Details**. For more information, refer to the [User History Details](#) section in this chapter.

3.6.3 Top Categories

The **Top Categories** report displays the amount of bandwidth consumed by categories of visited websites on a specific date.



Bandwidth (DL/UL)	Web Category	Number of Sites	Number of Users
196.98 MB / 165.09 KB	WebMonitor Updates	45	1
3.02 MB / 88.13 KB	Business and Economy, Computer and Internet Info	7	2
2.07 MB / 115.2 KB	Search Engines	8	2
1.27 MB / 26.52 KB	Streaming Media	1	1
462.26 KB / 23.9 KB	Internet Portals	9	2
325.52 KB / 14.06 KB	Web Advertisements	8	2
194.25 KB / 8.33 KB	Computer and Internet Info	6	2
27.86 KB / 4.17 KB	Business and Economy	5	2
16.44 KB / 19.45 KB	News and Media, Shopping, Streaming Media	1	2
14.88 KB / 2.53 KB	Internet Portals, Web Advertisements	1	2
1.51 KB / 1.27 KB	Local Information, News and Media	1	1
1.49 KB / 2.21 KB	Shareware and Freeware	1	1
1.01 KB / 1.2 KB	Parked Sites	1	1
0 B / 321 B	Unknown	1	1

Screenshot 18 - Bandwidth Consumption: Top Categories report

Navigate to **Monitoring ► Bandwidth Consumption ► Top Categories** to access the **Top Categories** report.

The information displayed includes:

- **Bandwidth (DL/UL)** - the total bandwidth used by each web category
- **Web Category** - the classification of which the accessed sites form part of
- **Number of Sites** - the number of sites that were accessed by the users, which form part of the category
- **Number of Users** - the number of users that accessed the sites which form part of the category

Table Sorting

By default, the list is sorted by **Bandwidth (DL)** in descending order, but all columns can be sorted in either ascending or descending order by clicking on the appropriate column heading.

Further Information

Select the **Web Category** hyperlink to view the details for the web category. The information displayed includes:

- **Site** - the site that was accessed by the users
- **User/IP** - the user/IP that is being monitored
- **Bandwidth (DL/UL)** - the total bandwidth used by each site
- **Hits** - the total number of requests (more than one request can be submitted for the same site) by the user

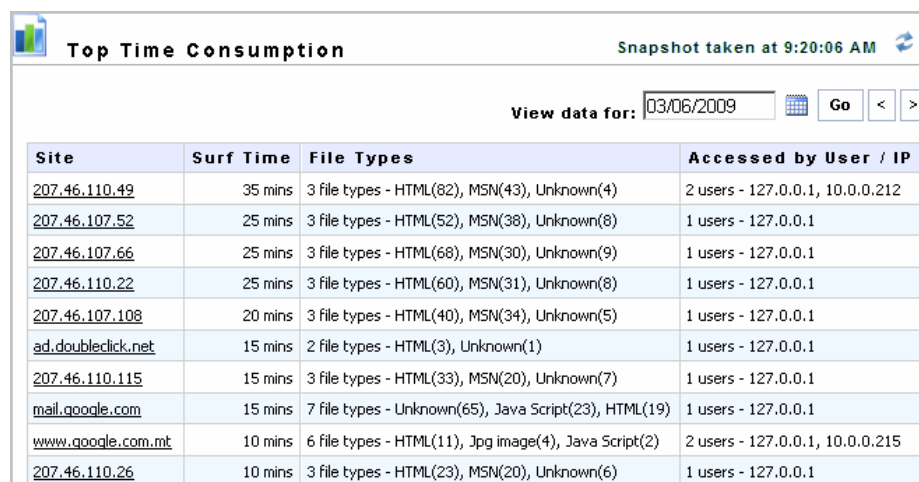
3.7 Sites History

The **Sites History** reports allows you to monitor total browsing times per site and the number of times a site was accessed. Two types of reports are available:

- Top Time Consumption
- Top Hits Count

3.7.1 Top Time Consumption

The **Top Time Consumption** report lists the sites on which network users spent most time browsing a site on a specific date.



Site	Surf Time	File Types	Accessed by User / IP
207.46.110.49	35 mins	3 file types - HTML(82), MSN(43), Unknown(4)	2 users - 127.0.0.1, 10.0.0.212
207.46.107.52	25 mins	3 file types - HTML(52), MSN(38), Unknown(8)	1 users - 127.0.0.1
207.46.107.66	25 mins	3 file types - HTML(66), MSN(30), Unknown(9)	1 users - 127.0.0.1
207.46.110.22	25 mins	3 file types - HTML(60), MSN(31), Unknown(8)	1 users - 127.0.0.1
207.46.107.108	20 mins	3 file types - HTML(40), MSN(34), Unknown(5)	1 users - 127.0.0.1
ad.doubleclick.net	15 mins	2 file types - HTML(3), Unknown(1)	1 users - 127.0.0.1
207.46.110.115	15 mins	3 file types - HTML(33), MSN(20), Unknown(7)	1 users - 127.0.0.1
mail.google.com	15 mins	7 file types - Unknown(65), Java Script(23), HTML(19)	1 users - 127.0.0.1
www.google.com.mt	10 mins	6 file types - HTML(11), Jpg image(4), Java Script(2)	2 users - 127.0.0.1, 10.0.0.215
207.46.110.26	10 mins	3 file types - HTML(23), MSN(20), Unknown(6)	1 users - 127.0.0.1

Screenshot 19 - Sites History: Top Time Consumption report

Navigate to **Monitoring ► Sites History ► Top Time Consumption** to access the **Top Time Consumption** report.

The information displayed includes:

- **Site** - the site that was accessed by the users
- **Surf Time** - the total time spent browsing each site
- **File Types** - the total number of and the types of files accessed from each site followed by the number of times each file type was accessed in brackets
- **Accessed by User / IP** - the total number and names/IP addresses of users/IP addresses that accessed the site

Table Sorting



By default, the list is sorted by **Surf Time** in descending order, but all columns apart from **File Types** and **Accessed by User / IP** can be sorted in either ascending or descending order by clicking on the appropriate column heading.

Further Information

Select the **Site** hyperlink to view the **Site Access History**. For more information, refer to the [Site Access History](#) section in this chapter.

3.7.2 Top Hits Count

The **Top Hits Count** report lists the sites that were most frequently accessed by network users on a specific date.

 **Top Hits Count** Snapshot taken at 2:45:05 PM 

Show Hits Over Time Charts View data for:

Site	Hits	File Types	Accessed by User / IP
update.gfi.com	76	3 file types - unknown(21), html(19), zip(1)	1 users - 127.0.0.1
www.google.com	70	5 file types - unknown(2), html(43), gif(10), j.script(4), png(2)	2 users - 127.0.0.1, 10.0.0.212
www.bay.com.mt	67	6 file types - html(2), jpg(11), gif(42), flash(1), css(3), j.script(3)	1 users - 127.0.0.1
l.vimq.com	49	6 file types - unknown(1), jpg(10), gif(4), css(7), j.script(14), png(2)	1 users - 10.0.0.212
i3.microsoft.com	43	3 file types - jpg(2), j.script(10), png(20)	2 users - 10.0.0.212, 127.0.0.1
col.stb.s-msn.com	42	2 file types - jpg(20), gif(1)	1 users - 10.0.0.212
i.microsoft.com	39	3 file types - jpg(2), gif(4), png(21)	2 users - 10.0.0.212, 127.0.0.1

Screenshot 20 - Sites History: Top Hits Count report

Navigate to **Monitoring ► Sites History ► Top Hits Count** to access the **Top Hits Count** report.

The information displayed includes:

- **Show Hits Over Time Chart** - for more information, refer to the [Charts](#) section in this chapter.
- **Site** - the site that was accessed by the users
- **Hits** - the total number of requests (more than one request can be submitted for the same site) by the user
- **File Types** - the total number of and the types of files accessed from each site followed by the number of times each file type was accessed in brackets
- **Accessed by User / IP** - the total number and names/IP addresses of users/IP addresses that accessed the site

Table Sorting

By default, the list is sorted by **Hits** in descending order, but all columns apart from **File Types** and **Accessed by User / IP** can be sorted in either ascending or descending order by clicking on the appropriate column heading.

Further Information

Select the **Site** hyperlink to view the **Site Access History**. For more information, refer to the [Site Access History](#) section in this chapter.

3.8 Users History

The **Users History** reports allows you to monitor total browsing time per user, total number of times a user accesses sites and total number of policy violations per user. Three types of reports are available:

- Top Surfers
- Top Hits Count
- Top Policy Breakers

3.8.1 Top Surfers

The **Top Surfers** report lists the time spent by network users browsing sites on a specific date.

User / IP	Surf Time	Sites Accessed
clint2\msn_messenger	2 hr 25 mins	52 sites - 207.46.107.108, 207.46.107.52, 207.46.107.66, 207.46.110.115
clint2\administrator	50 mins	30 sites - 88.198.39.17, ajax.googleapis.com, b.mail.google.com, chatenab
127.0.0.1	5 mins	6 sites - update.gfi.com, update009.gfi.com, update032.gfi.com, update039.gfi.com, u
217.65.100.89	0 mins	1 sites - /w00tw00t.at.isc.sans.dfind:)
10.0.0.212	0 mins	3 sites - loginnet.passport.com, packetscreen.com, rsi.hotmail.com
194.158.59.141	0 mins	1 sites - beta.bpftpsrver.com
10.0.0.213	0 mins	5 sites - ajax.googleapis.com, mail.google.com, ssl.google-analytics.com, ww

Screenshot 21 - Users History: Top Surfers report

Navigate to **Monitoring ► Users History ► Top Surfers** to access the **Top Surfers** report.

The information displayed includes:

- **User/IP** - the user/IP that is being monitored
- **Surf Time** - the total time spent browsing each site
- **Sites Accessed** - the total number and names of different sites accessed by the user

Table Sorting

By default, the list is sorted by **Surf Time** in descending order, but all columns apart from **Sites Accessed** can be sorted in either ascending or descending order by clicking on the appropriate column heading.

Further Information

Select the **User/IP** hyperlink to view the **User History Details**. For more information, refer to the [User History Details](#) section in this chapter.

3.8.2 Top Hits Count

The **Top Hits Count** report, lists the users with the highest number of site accesses on a specific date.

User / IP	Hits	Sites Accessed
clint2\msn_messenger	981	52 sites - 207.46.107.108, 207.46.107.52, 207.46.107.66, 207.46.110.115, 207.46.11
clint2\administrator	418	30 sites - 88.198.39.17, ajax.googleapis.com, b.mail.google.com, chatenabled.mail.goo
127.0.0.1	185	6 sites - update.gfi.com, update009.gfi.com, update032.gfi.com, update039.gfi.com, u
10.0.0.212	43	3 sites - loginnet.passport.com, packetscreen.com, rsi.hotmail.com
10.0.0.213	28	5 sites - ajax.googleapis.com, mail.google.com, ssl.google-analytics.com, www.google.c
217.65.100.89	1	1 sites - /w00tw00t.at.isc.sans.dfind:)
194.158.59.141	1	1 sites - beta.bpftpsrver.com

Screenshot 22 - Users History: Top Hits Count report

Navigate to **Monitoring ► Users History ► Top Hits Count** to access the **Top Hits Count** report.

The information displayed includes:

- **Show Hits Over Time Chart** - for more information, refer to the [Charts](#) section in this chapter.
- **User/IP** - the user/IP that is being monitored
- **Hits** - the total number of requests (more than one request can be submitted for the same site) by the user
- **Sites Accessed** - the total number and names of different sites accessed by the user

Table Sorting

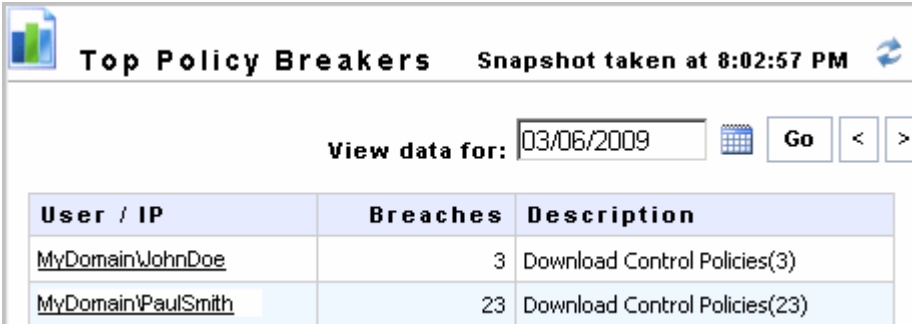
By default, the list is sorted by **Hits** in descending order, but all columns apart from **Sites Accessed** can be sorted in either ascending or descending order by clicking on the appropriate column heading.

Further Information

Select the **User/IP** hyperlink to view the **User History Details**. For more information, refer to the [User History Details](#) section in this chapter.

3.8.3 Top Policy Breakers

The **Top Policy Breakers** report, lists the users with the highest number of policy violations on a specific date.



User / IP	Breaches	Description
MyDomain\JohnDoe	3	Download Control Policies(3)
MyDomain\PaulSmith	23	Download Control Policies(23)

Screenshot 23 - Users History: Top Policy Breakers report

Navigate to **Monitoring ► Users History ► Top Policy Breakers** to access the **Top Policy Breakers** report.

The information displayed includes:

- **User/IP** - the user/IP that is being monitored and who violated the policy
- **Breaches** - the number of policy violations by the user
- **Description** - the category of the violated policy followed by the number of times the policy has been broken

Table Sorting

The list is sorted by **User/IP** in ascending order.

Further Information

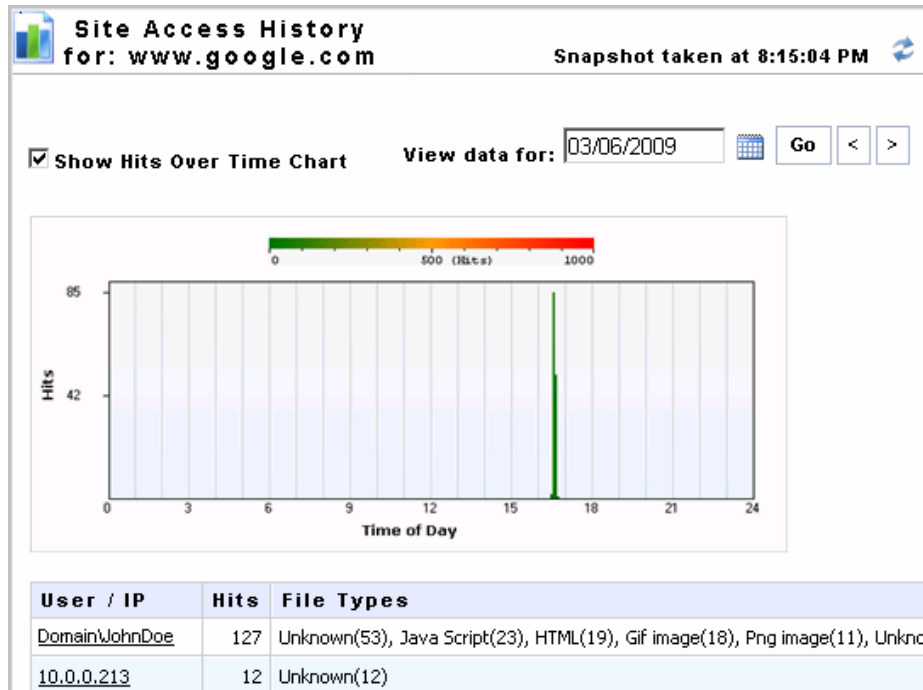
Select the **User/IP** hyperlink to view the details for the user/IP address. The information displayed includes:

- **Time** - the time the violation occurred
- **Description** - the specific name of the violated policy
- **URL** - the URL of the unauthorized site

- **IP** - the IP address that accessed the site

3.9 Site Access History

The **Site Access History** view graphically represents and lists details related to an accessed site on a specific date.



Screenshot 24 - Site Access History view

1. To access the Site Access History view:

- Option 1: Navigate to **Monitoring ► Bandwidth Consumption ► Top Sites** to access the **Top Sites** report.
- Option 2: Navigate to **Monitoring ► Sites History ► Top Time Consumption** to access the **Top Time Consumption** report.
- Option 3: Navigate to **Monitoring ► Sites History ► Top Hits Count** to access the **Top Hits Count** report.

2. Select the **Site** hyperlink.

The information displayed includes:

- **Show Traffic Over Time Chart** - for more information, refer to the [Charts](#) section in this chapter.
- **Show Hits Over Time Chart** - for more information, refer to the [Charts](#) section in this chapter.
- **User/IP** - the user/IP that is being monitored
- **Usage (DL/UL)** - the total bandwidth used by each user. Hover on a specific value to view a Download/Upload Traffic over a 24-hour chart for a specific site, date and user.
- **Hits** - the total number of requests (more than one request can be submitted for the same site) by the user. Hover on a specific value to view a Hits over a 24-hour chart for a specific site, date and user.
- **File Types** - the types of files accessed by each user followed by the number of times the file type was accessed in brackets. Hover on a specific value (a site might have more than one file type value

listed) to view a Download/Upload Traffic over a 24-hour chart for a specific site, date and user.

Table Sorting

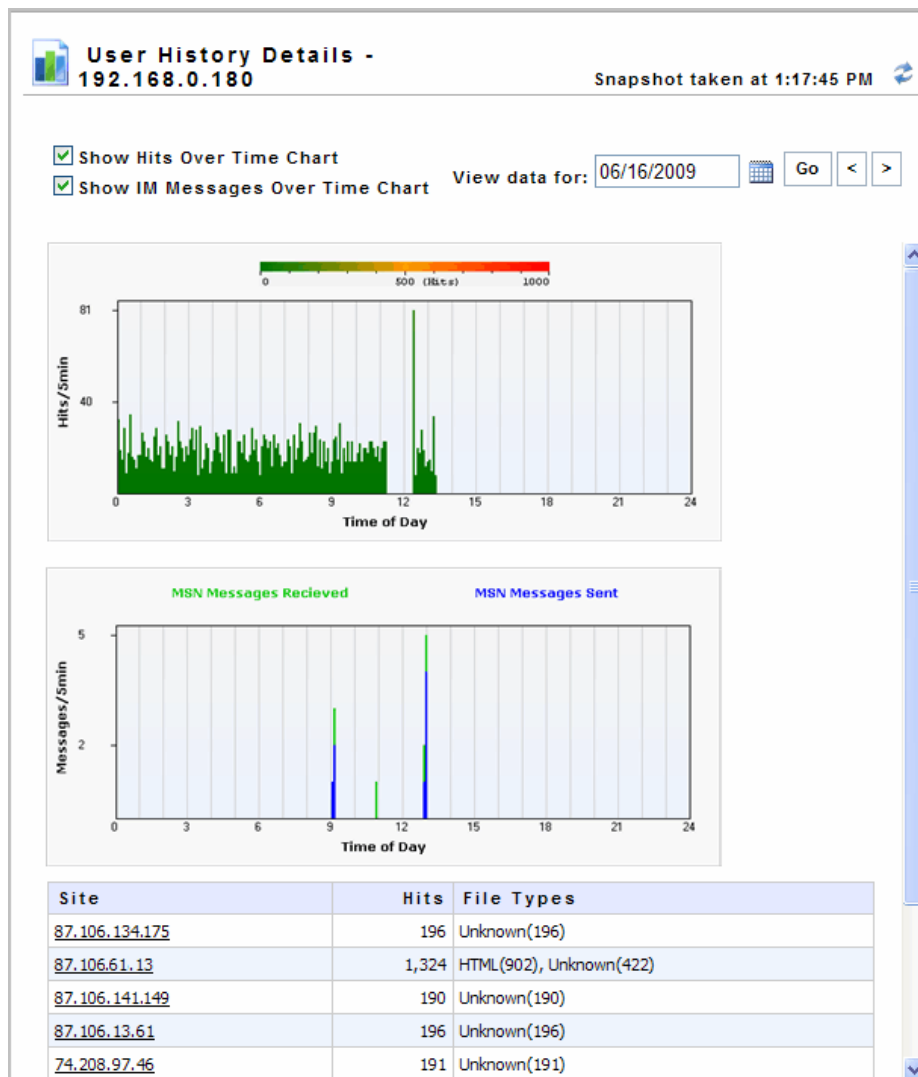
By default, the list is sorted by **Hits** in descending order, but all columns apart from **File Types** can be sorted in either ascending or descending order by clicking on the appropriate column heading.

Further Information

Select the **User/IP** hyperlink to view the **User History Details**. For more information, refer to the [User History Details](#) section in this chapter.

3.10 User History Details

The **User History Details** view graphically represents and lists details related to a monitored user/IP of a specific date.



Screenshot 25 - User History Details view

1. To access the User History Details view:
 - Option 1: Navigate to **Monitoring** ► **Bandwidth Consumption** ► **Top Users** to access the **Top Users** report.
 - Option 2: Navigate to **Monitoring** ► **Users History** ► **Top Surfers** to access the **Top Surfers** report.

- Option 3: Navigate to **Monitoring ► Users History ► Top Hits Count** to access the **Top Hits Count** report.

2. Select the **User/IP** hyperlink.

The information displayed includes:

- **Show Traffic Over Time Chart** - for more information, refer to the [Charts](#) section in this chapter.
- **Show Hits Over Time Chart** - for more information, refer to the [Charts](#) section in this chapter.
- **Show IM Messages Over Time Chart** - for more information, refer to the [Charts](#) section in this chapter.
- **Site** - the site that was accessed by the users
- **Usage (DL/UL)** - the total bandwidth used by each user. Hover on a specific value to view a Download/Upload Traffic over a 24-hour chart for a specific user, date and site.
- **Hits** - the total number of requests (more than one request can be submitted for the same site) by the user. Hover on a specific value to view a Hits over a 24-hour chart for a specific user, date and site.
- **File Types** - the types of files accessed by each user followed by the number of times the file type was accessed in brackets. Hover on a specific value (a site might have more than one file type value listed) to view a Download/Upload Traffic over a 24-hour chart for a specific user, date and site.
- **Web Category** - the classification of which the accessed site forms part of

Table Sorting

By default, the list is sorted by **Hits** in descending order, but all columns apart from **File Types** can be sorted in either ascending or descending order by clicking on the appropriate column heading.

Further Information

Select the **Site** hyperlink to view the **Site Access History**. For more information, refer to the [Site Access History](#) section in this chapter.

3.11 Activity Log

The **Activity Log** report allows monitoring items that have been blocked or quarantined and processes that have failed on a specific date.

User	Time	Description	URL
MyDomain\JoeDoe	16:28:52	Default Download Control Policy	http://mail.google.com/
Domain\JaneSmith	16:16:52	Default Download Control Policy	http://intl.video.msn.com/s/us/i/im.png
Domain\MaryJohnson	16:16:51	Default Download Control Policy	http://images.match.com/match/msn/me:
MyDomain\KateBlack	15:41:01	Default IM Control Policy	http://gateway.messenger.hotmail.com/h
MyDomain\PaulSmith	15:39:39	Default IM Control Policy	http://gateway.messenger.hotmail.com/h
Domain\TomBrown	14:35:29	Default Download Control Policy	http://www.google.com/search?q=cann

Screenshot 26 - Activity Log view

Navigate to **Monitoring ► Activity Log** to access the **Activity Log** view.

The information displayed includes:


- **User** - the user/IP that is being monitored
- **Time** - the time the violation occurred
- **Description** - the name of the violated policy
- **URL** - the URL of the unauthorized site

Table Sorting




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

3.12 Viewing data by date

By default, all reports within the **Bandwidth Consumption**, **Sites History**, **Users History** and **Activity Log** nodes list data for the current day (from midnight to the instant the report is launched).

The displayed information is not refreshed automatically, as a result new data that becomes available after the generation of the current day report, is not displayed automatically. To update such data, click the refresh button  at the upper right corner of the view.

To view data for other days, use the controls at the upper right of the view:

- **Previous day** - click the back button .
- **Next day** - click the forward button .
- **Specific date** - click the calendar button , select the required date and click **Go** to retrieve data for that date.

NOTE: If no data for a specific date is available (e.g. a future date is selected), an error message stating that data was unable to be retrieved is displayed.

3.13 Charts

Charts allow you to monitor statistics in an easier way. Three types of graphical representations are available:

- Show Traffic Over Time Chart
- Show Hits Over Time Charts

- Show IM Messages Over Time Chart

Show Traffic Over Time Chart

This chart allows you to view a graphical representation of the flow of total Download/Upload Traffic over a 24-hour period for a selected date.

This chart also allows you to identify peaks in Download/Upload Traffic generated by the users.

Show Hits Over Time Charts

This chart allows you to view a graphical representation of the flow of total number of Hits over a 24-hour period for a selected date.

This chart also allows you to identify peaks in the amount of requests by the users.

Show IM Messages Over Time Chart

This chart allows you to view a graphical representation of the flow of total number of Instant Messages over a 24-hour period for a selected date.

This chart also allows you to identify peaks in the amount of Instant Messages sent/received by the users.

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.

IMPORTANT: 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 27 - 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).

NOTE: When adding a **User** to the whitelist, specify the username in the format DOMAIN\user.


NOTE: When adding a **Site** to the whitelist, you can use wildcards (e.g. "*.website.com"). For more information, refer to the [Using wildcards](#) section in this chapter.

3. Click **Save Settings** to finalize setup.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

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 you want to delete.
3. Click **Save Settings** to complete deletion of whitelist items.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

4.2.4 Adding items to the Temporary Whitelist

The screenshot shows the 'Whitelist' configuration window. At the top, there is a 'Whitelist' title bar with a green checkmark icon and two buttons: 'Save Settings' and 'Cancel'. Below the title bar, there is a paragraph of text: '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.' Below this text are two tabs: 'Permanent Whitelist' and 'Temporary Whitelist', with the latter being selected. Under the 'Temporary Whitelist' tab, there is another paragraph: '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.' Below this is an 'Add' button. A table with four columns is shown: 'Grant To', 'Access To', 'For (hours)', and a trash icon column. The table contains two rows of data. Below the table is a 'Delete All' button.

Grant To	Access To	For (hours)	
192.168.7.88	mail.google.com	2,400.0	
192.168.5.24	www.gfi.com	24.0	

Screenshot 28 - 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**.

The screenshot shows the 'Grant Temporary Access' dialog box. It has a title bar with a close button (X). The dialog contains three sections: 'Grant to:' with a dropdown menu set to 'IP' and a text box containing '192.168.5.88'; 'Access to:' with a text box containing '*.msn.com'; and 'For:' with a text box containing '5' and the word 'hours'. At the bottom, there are two buttons: 'Add' and 'Cancel'.

Screenshot 29 - Temporary Whitelist: Granting Temporary Access dialog

3. From the **Grant to:** drop-down list, select whether a User or an IP will be added to the temporary whitelist and provide the user or IP to be granted temporary access as well as the URL of the site and the number of hours.

NOTE: When granting temporary access to a user, specify the username in the format DOMAIN\user.

NOTE: When adding a **Site** to the whitelist, you can use wildcards (e.g. "*.website.com"). For more information, refer to the [Using wildcards](#) section in this chapter.

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

5. Click **Save Settings** to finalize setup.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.


NOTE: The number of hours during which the user or IP has access to a site become applicable from the moment **Save Settings** is clicked.

NOTE: Time remaining before access is revoked can be viewed in the **For (hours)** column in the **Temporary Whitelist** view.

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 you want to delete.

3. Click **Save Settings** to complete deletion of whitelist items.

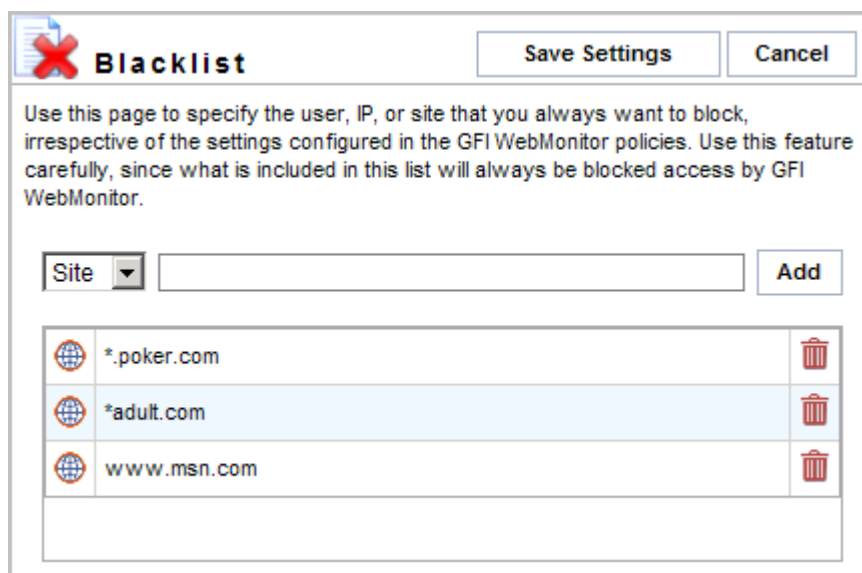
NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.







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.

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

4.3.1 Adding items to the Blacklist



Blacklist		Save Settings	Cancel
Use this page to specify the user, IP, or site that you always want to block, irrespective of the settings configured in the GFI WebMonitor policies. Use this feature carefully, since what is included in this list will always be blocked access by GFI WebMonitor.			
Site	<input type="text"/>	Add	
	*poker.com		
	*adult.com		
	www.msn.com		

Screenshot 30 - 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).

NOTE: When adding a **User** to the blacklist, specify the username in the format DOMAIN\user.


NOTE: When adding a **Site** to the blacklist, you can use wildcards (e.g. "*.website.com"). For more information, refer to the [Using wildcards](#) section in this chapter.

3. Click **Save Settings** to finalize setup.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

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 you want to delete.
3. Click **Save Settings** to complete deletion of blacklist items.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

4.4 Using wildcards

When adding a site to the whitelist or blacklist, you can use wildcards 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 based on site categories together with the WebGrade database.

The category of a particular site is determined through the WebGrade Database; if a site is listed in the database, GFI WebMonitor then uses the configured web filtering policies to determine what action to take.


Policies can be customized to apply during specific periods. For example, a policy can enable users to access news and entertainment related sites during lunch breaks but not during working hours.

Pre-defined site categories include pornography, adult themes, games, violence and others. The database is updated on a regular basis and updates are automatically downloaded to GFI WebMonitor.



5.2 Web Filtering Policies

The **Web Filtering Policies** node allows 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 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:

- **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); i.e. upon the discretion of the administrator temporary access is allowed to blocked sites
- **Exclude** or **Include** specific sites per policy.

 **Web Filtering Policies**

Use this page to configure web filtering policies that allow you to manage access to the internet per user, group, or IP, based on site categories. GFI WebMonitor determines the category of a particular site by performing lookups in the WebGrade Database, and then uses this information in conjunction with the policies configured below. The policies are processed from top to bottom and the first one to match is applied.


Policy Name	Applies To	Enabled	
Default Web Filtering Policy	 Applies to everyone	<input checked="" type="checkbox"/>	

Screenshot 31 - Web Filtering Policies view

5.2.1 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**

Use this page to configure a web filtering policy.

Policy Name

Policy Description

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 32 - Web Filtering Policies: General tab


3. Select the **General** tab.
4. Provide a new policy name and description in the **Policy Name** field and the **Policy Description** text box respectively.
5. In the **Policy Schedule** area, specify the time period(s) during which the new policy will be enforced.

Screenshot 33 - Web Filtering Policies: Web Filtering tab

6. Select the **Web Filtering** tab and define the categories applicable to the new policy and the actions to take:

- Allow categories: Select categories from the **Blocked Categories** list and click **Allow>**.
- Block categories: Select categories from the **Allowed Categories** list and click **<Block**.
- Quarantine access: Select categories from the **Allowed Categories** list and click **<Quarantine**.

NOTE: Advanced category conditions can also be configured by selecting the **Show Advanced Options** button. For more information, refer to the [Configuring advanced Web Filtering Policy conditions](#) section in this chapter.

 **Web Filtering Policy** Save Settings Cancel







Use this page to configure a web filtering policy.

General **Web Filtering** **Exceptions** **Applies To**

Notifications

Excluded Sites





Add

	www.gfi.com	
	www.microsoft.com	
	www.gfisoftware.com	

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

Included Sites

Add

	www.facebook.com	
	www.hi5.com	

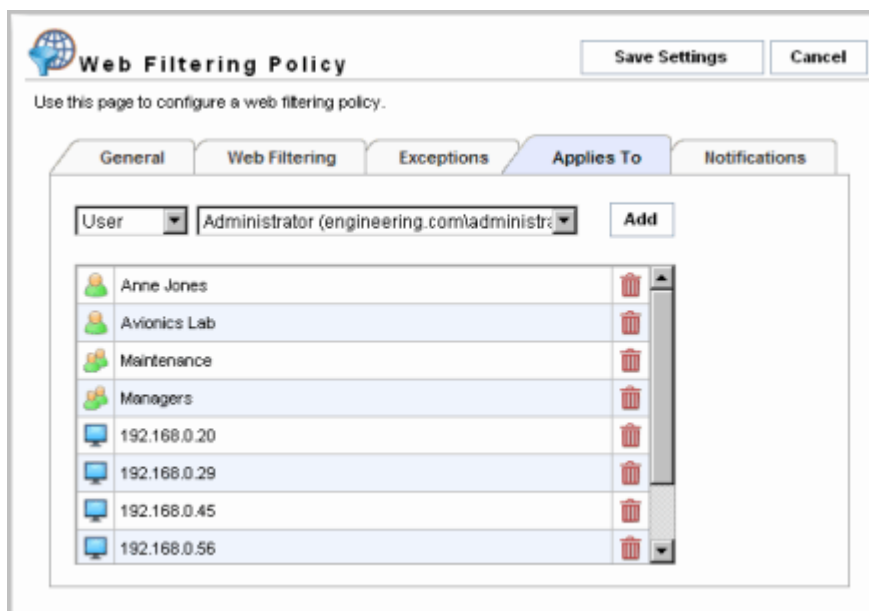
NOTE: The above sites will be **BLOCKED** by this policy, even when their category is not blocked in the Web Filtering tab.

Screenshot 34 - 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 (i.e. allowed) from the policy. This enables users to access sites overriding any policy setup.
- Included (i.e. blocked) in the new policy. The URLs specified in the included sites will be blocked regardless of the scope of the new policy.

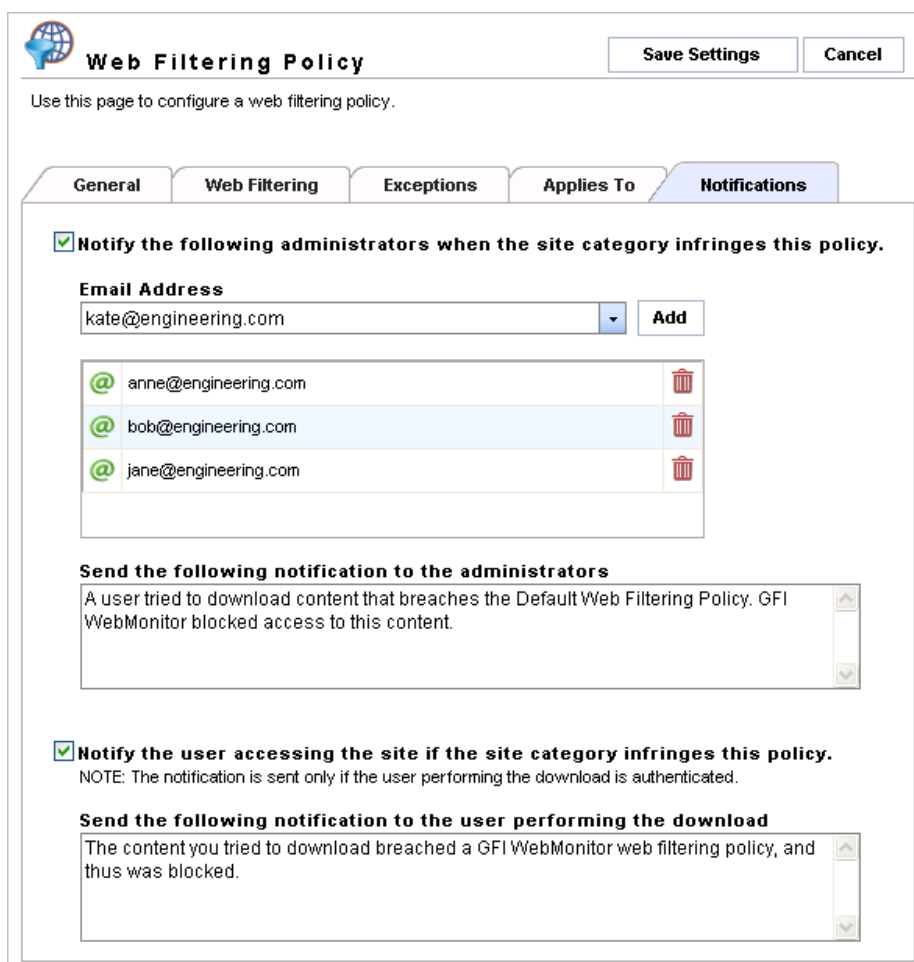
NOTE: The **Exceptions** tab is similar to a whitelist/blacklist feature that overrides any rules within the policy.



Screenshot 35 - 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).

NOTE: When adding a user, specify the username in the format DOMAIN\user.



Screenshot 36 - Web Filtering Policies: Notifications tab

9. (Optional) Select the **Notifications** tab and select the **Notify the following administrators when the site category infringes this**

policy checkbox to enable notification and define the administrator's notification email address and provide the body text of the notification email.

10. (Optional) Select the **Notify the user accessing the site if the site category infringes this policy** checkbox to enable notification and provide the body text of the notification email.


11. Click **Save Settings** to finalize creating a new policy. The new policy will now be listed in the main **Web Filtering Policies** view.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

5.2.2 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 you want to edit.

NOTE: For more information, refer to the [Adding a Web Filtering Policy](#) section in this chapter.

3. Click **Save Settings** to finalize editing a policy.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

5.2.3 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 you want to enable or disable.


3. Click **Save Settings** to finalize enabling or disabling a policy.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

5.2.4 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 you want to delete.

3. Click **Save Settings** to finalize deleting a policy.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

5.2.5 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.

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

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

5.3 Configuring advanced Web Filtering Policy conditions

The **Override Rules** area allows 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.

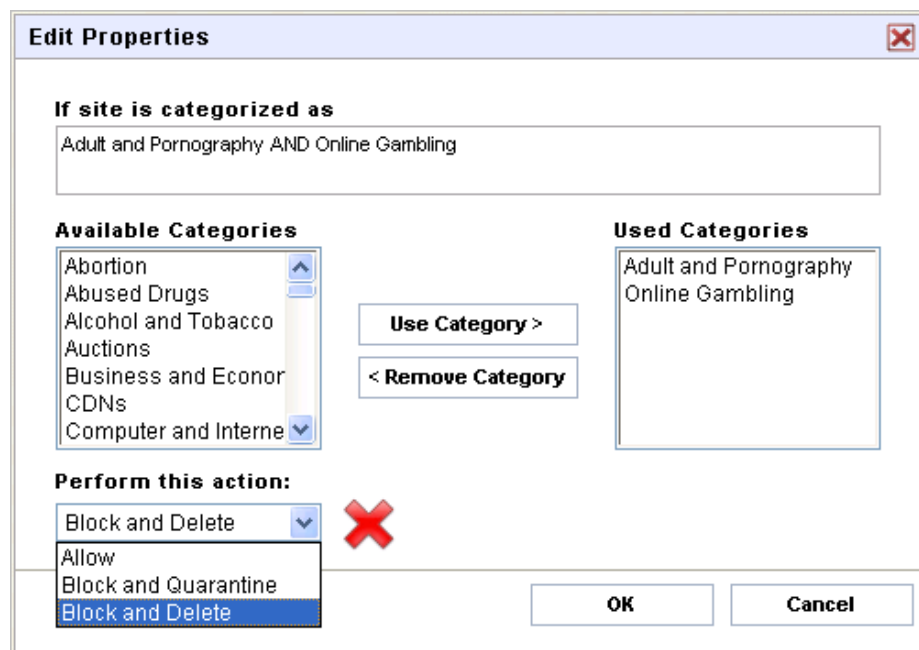
IMPORTANT: For a site to be blocked by an advanced condition, it must be listed under ALL categories defined in the condition.

IMPORTANT: These advanced Web Filtering Policy conditions take priority over categories specified in the Allowed Categories and Blocked Categories list boxes.

5.3.1 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.



Screenshot 37 - Adding an advanced Web Filtering Policy condition

2. Click the **Add Condition** button to view the **Edit Properties** dialog.
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 delete sites which fall under the categories 'Adult and Pornography' AND 'Online Gambling':

- a. Select **Adult and Pornography** from Available Categories list box and click Use Category
- b. Select **Online Gambling** from Available Categories list box and click Use Category
- c. Select **Block and Delete** 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 'Adult and Pornography' only and likewise it is NOT blocked if it is categorized as 'Online Gambling' only.

4. Click **Save Settings** to finalize creating an advanced condition for a policy.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

5.3.2 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** to finalize editing an advanced condition for a policy.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

5.3.3 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 you want to delete.
3. Click **Save Settings** to finalize deleting an advanced condition for a policy.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

5.4 WebGrade Database

The **WebGrade Database** node allows 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

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 full version 1.329.
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: 2009-06-25 03:09 Up-to-date. Next update: 2009-06-25 12:09

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.

Screenshot 38 - Web Filtering Policies: WebGrade Database view

5.4.1 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.

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

3. Click **Save Settings** to finalize enabling or disabling the database.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

5.4.2 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.

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

3. Click **Save Settings** to finalize enabling or disabling online lookups for URLs.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

5.4.3 Configuring WebGrade Database Updates

The **WebGrade Database Updates** area allows 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** to finalize configuration of settings for the WebGrade Database to update automatically.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

5.4.4 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
3. 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 WebSecurity Edition - File scanning and download control

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:

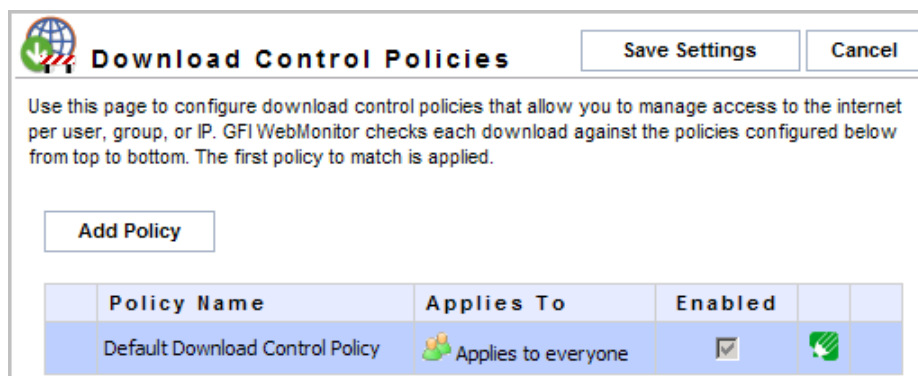
- **Download Control Policies:** to control software downloads
- **IM (Instant Messaging) Control Policies:** to control access and use of MSN / Microsoft Windows Live Messenger
- **Virus Scanning Policies:** to configure which downloaded files should be scanned for viruses and spyware
- **Anti-Phishing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

6.2 Download Control Policies

The **Download Control Policies** node allows 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 by user(s), group(s) and/or IP(s)
- Block the file from being downloaded by user(s), group(s) and/or IP(s) and quarantine the downloaded file
- Block the file from being downloaded by user(s), group(s) and/or IP(s) and delete the downloaded file

NOTE: For allowed downloads, GFI WebMonitor then applies the configured **Virus Scanning Policies** and determines its virus scanning options.



Screenshot 39 - 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 the 'Download Control Policy' configuration page with the 'General' tab selected. The page title is 'Download Control Policy' and it includes 'Save Settings' and 'Cancel' buttons. Below the title is the instruction: 'Use this page to configure a download control policy.' The 'General' tab is active, showing a 'Policy Name' text box with the value 'New Policy Name' and a 'Policy Description' text area with the value 'New Policy Description'. Other tabs visible are 'Download Control', 'Applies To', and 'Notifications'.

Screenshot 40 - Download Control Policies: General tab

3. Select the **General** tab.

4. Key in a new policy name and description in the **Policy Name** field and the **Policy Description** text boxes respectively.

The screenshot shows the 'Download Control Policy' configuration page with the 'Download Control' tab selected. The page title is 'Download Control Policy' and it includes 'Save Settings' and 'Cancel' buttons. Below the title is the instruction: 'Use this page to configure a download control policy.' The 'Download Control' tab is active, displaying a table of file types and their actions. Below the table are four buttons: 'Allow All', 'Add Content-type', 'Block and Delete All', and 'Block and Quarantine All'.

Action	File Type
✓	Html
+	Jpg image
+	Gif image
✓	Flash
✗	CSS
✓	XML .xml .xsl
✓	Javascript
✓	Zip
✗	Executable
✗	RAR archive
✓	Word .doc

Screenshot 41 - Download Control Policies: Download Control tab

5. Select the **Download Control** tab.

Change Action

File Type: Jpg image

Content-type

image/jpeg
image/pjpeg

Description

Files which have their HTTP header Content-type image/jpeg image/pjpeg OR their signature recognized as that of a Jpg image file.

Perform this action:

Block and Quarantine

OK Cancel

Screenshot 42 - Adding a new content type dialog

6. Click any **File Type** hyperlink from the list to display the **Change Action** dialog and configure the actions to be taken for that file type.

7. From the **Perform this action** drop-down list select the applicable action to be taken. The available options are:

- Allow
- Block and Quarantine
- Block and Delete

8. Click **OK** to apply the action.

9. (Optional) Click the **Add Content-type** button to create a new definition. 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

Anne Jones	
John Doe	
Maintenance	

Screenshot 43 - Download Control Policies: Applies To tab

10. 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).

NOTE: When adding a user, specify the username in the format DOMAIN\user.

The screenshot shows the 'Download Control Policy' configuration window with the 'Notifications' tab selected. The window title is 'Download Control Policy' and it has 'Save Settings' and 'Cancel' buttons. Below the title bar, there is a sub-header 'Use this page to configure a download control policy.' and four tabs: 'General', 'Download Control', 'Applies To', and 'Notifications'. The 'Notifications' tab is active and contains the following elements:

- A checked checkbox labeled 'Notify the following administrators when the downloaded content infringes this policy.'
- An 'Email Address' input field with a dropdown arrow and an 'Add' button.
- A list of email addresses, currently containing 'Administrator@clint2.local' with a trash icon to its right.
- A section titled 'Send the following notification to the administrators' with a text area containing the message: 'A user tried to download content that breaches a download control policy. GFI WebMonitor blocked access to this content.'
- A checked checkbox labeled 'Notify the user performing the download when the downloaded content infringes this policy.'
- A note: 'NOTE: The notification is sent only if the user performing the download is authenticated.'
- A section titled 'Send the following notification to the user performing the download' with a text area containing the message: 'The content you tried to download breached a GFI WebMonitor download control policy, and thus was blocked.'

Screenshot 44 - Download Control Policies: Notifications tab

11. (Optional) Select the **Notifications** tab and select the **Notify the following administrators when the downloaded content infringes this policy** checkbox to enable notification and define the administrator's notification email address and provide the body text of the notification email.


12. (Optional) Select the **Notify the user performing the download when the downloaded content infringes this policy** checkbox to enable notification and provide the body text of the notification email.

13. Click **Save Settings** to finalize creating a new policy. The new policy will now be listed in the main **Download Control Policies** view.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

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 you want to edit.

NOTE: For more information, refer to the [Adding a Download Control Policy](#) section in this chapter.

3. Click **Save Settings** to finalize editing a policy.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

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 you want to enable or disable.
3. Click **Save Settings** to finalize enabling or disabling a policy.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

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 you want to delete.
3. Click **Save Settings** to finalize deleting a policy.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

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.

IMPORTANT: All added Download Control Policies take priority over the Default Download Control Policy.

NOTE: 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 allows you to create new definitions for file types, which are not yet in the predefined list.

Screenshot 45 - 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** to finalize creating a new content-type.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

6.3 IM (Instant Messaging) Control Policies

The **IM (Instant Messaging) Control Policies** node allows 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 the usage of a file triggers a policy, 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

Policy Name	Applies To	Enabled	
Default IM Control Policy	Applies to everyone	<input checked="" type="checkbox"/>	

Screenshot 46 - IM Control Policies view

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**.

The screenshot shows the 'IM Control Policy' configuration page. At the top, there is a title bar with a green speech bubble icon, the text 'IM Control Policy', and two buttons: 'Save Settings' and 'Cancel'. Below the title bar is a paragraph of instructions: '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.' Below the instructions are four tabs: 'General', 'IM Control', 'Applies To', and 'Notifications'. The 'General' tab is selected. Under the 'General' tab, there are two fields: 'Policy Name' with the text 'Administrators and Managers' and 'Policy Description' with the text 'Managers and Administrators are allowed to use MSN / Windows Live Messenger. (but not outgoing file transfers)'. The 'Policy Description' field has a vertical scrollbar on the right side.


Screenshot 47 - IM Control Policies: General tab

3. Select the **General** tab.
4. Provide a new policy name and description in the **Policy Name** field and the **Policy Description** text box respectively.

The screenshot shows the 'IM Control Policy' configuration page. At the top, there is a title bar with a green speech bubble icon, the text 'IM Control Policy', and two buttons: 'Save Settings' and 'Cancel'. Below the title bar is a paragraph of instructions: '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.' Below the instructions are four tabs: 'General', 'IM Control', 'Applies To', and 'Notifications'. The 'IM Control' tab is selected. Under the 'IM Control' tab, there are two radio button options: 'Block All MSN / Windows Live Messenger traffic' (with a red 'X' icon and an unselected radio button) and 'Allow MSN / Windows Live Messenger traffic' (with a green checkmark icon and a selected radio button).

Screenshot 48 - IM Control Policies: IM Control tab

5. Select the **IM Control** tab and define the actions to take. The available options are:
 - Block All MSN / Windows Live Messenger traffic
 - Allow MSN / Windows Live Messenger traffic



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

Specify users, groups or IPs to which this IM policy applies.

User

Add

	10.0.0.210	
	10.0.0.215	
	Anne Brown	
	JohnDoe	
	network_administrators	

NOTE: To apply settings to all users you must edit the Default IM Policy

Screenshot 49 - IM Control Policies: Applies To tab

6. 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).

NOTE: When adding a user, specify the username in the format DOMAIN\user.

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@127.0.0.1	
	Administrator@masterdomain.com	

Send the following notification to the administrators

A user tried to use instant messaging communications that breaches an IM control policy, GFI WebMonitor blocked access to this content.

IM Control policy breached: (Replace enclosed text with this policy name)

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

The instant messaging service you tried to use breached a GFI WebMonitor IM Control Policy, and thus was blocked.

Screenshot 50 - IM Control Policies: Notifications tab

7. (Optional) Select the **Notifications** tab and select the **Notify the following administrators when this IM policy is breached** checkbox to enable notification and define the administrator's notification email address and provide the body text of the notification email.

8. (Optional) Select the **Notify the user breaching this IM policy** checkbox to enable notification and provide the body text of the notification email.

9. Click **Save Settings** to finalize creating a new policy. The new policy will now be listed in the main **IM Control Policies** view.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

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 you want to edit.

NOTE: For more information, refer to the [Adding an IM Control Policy](#) section in this chapter.

3. Click **Save Settings** to finalize editing a policy.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

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 you want to enable or disable.
3. Click **Save Settings** to finalize enabling or disabling a policy.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

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 you want to delete.
3. Click **Save Settings** to finalize deleting a policy.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

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.

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

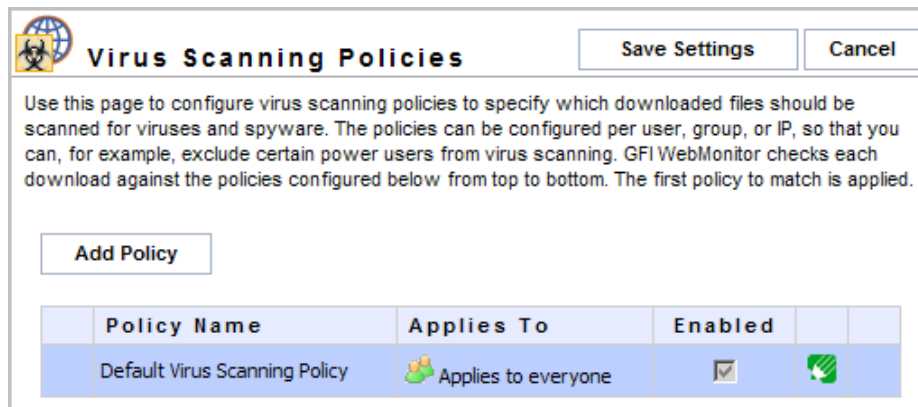
NOTE: Certain fields in the default policy cannot be edited. These include **Policy Name**, **Policy Description** and fields in the **Applies To** tab.

6.4 Virus Scanning Policies

The **Virus Scanning Policies** node allows 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 by user(s), group(s) and/or IP(s)
- Block the file from being downloaded by user(s), group(s) and/or IP(s) and quarantine the downloaded file
- Block the file from being downloaded by user(s), group(s) and/or IP(s) 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.

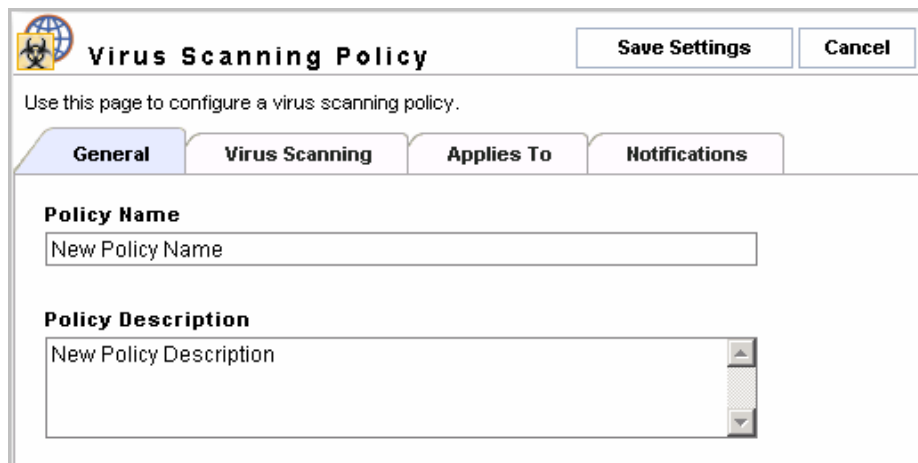


Screenshot 51 - Virus Scanning Policies view

6.4.1 Adding a Virus Scanning Policy

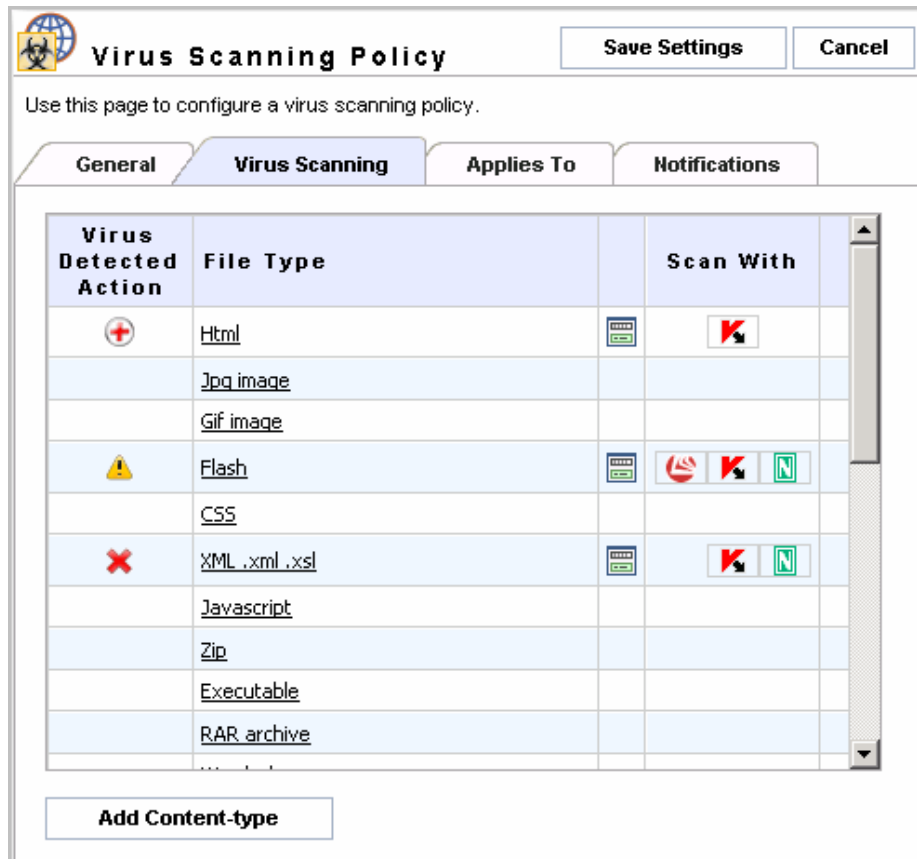
To add a Virus Scanning Policy:

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



Screenshot 52 - Virus Scanning Policies: General tab

3. Click the **General** tab.
4. Provide new policy name and description in the **Policy Name** field and the **Policy Description** text box respectively.



Screenshot 53 - Virus Scanning Policies: Virus Scanning tab

5. Select the **Virus Scanning** tab.
6. Click any **File Type** hyperlink from the list to display the **Select Virus Scanners and Action** dialog and configure the actions to be taken for that file type.
7. From the **If a virus is found perform this action:** drop-down list select the applicable action to be taken. The available options are:
 - Warn and Allow
 - Block and Quarantine
 - Block and Delete
8. Click **OK** to apply the action.
9. (Optional) Click the **Add Content-type** button to create a new definition. 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.

IP Add

	192.168.1.55	
	john doe	

Screenshot 54 - Virus Scanning Policies: Applies To tab

10. 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).

NOTE: When adding a user, specify the username in the format DOMAIN\user.

Virus Scanning Policy Save Settings Cancel

Use this page to configure a virus scanning policy.

General **Virus Scanning** **Applies To** **Notifications**

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

Email Address

Add

	Administrator@mydomain.com	
--	----------------------------	--

Send the following notification to the administrators

A user tried to download content that breaches a virus scanning policy. GFI WebMonitor blocked access to this content.

Content breached the following policy: (Replace enclosed text with this policy name)

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 or the IP is mapped.

Send the following notification to the user performing the download

The content you tried to download breached a GFI WebMonitor virus scanning policy, and thus was blocked.

Screenshot 55 - Virus Scanning Policies: Notifications tab

11. (Optional) Select the **Notifications** tab and select the **Notify the following administrators when the downloaded content infringes this policy** checkbox to enable notification and define the administrator's notification email address and provide the body text of the notification email.

12. (Optional) Select the **Notify the user performing the download when the downloaded content infringes this policy** checkbox to enable notification and provide the body text of the notification email.


13. Click **Save Settings** to finalize creating a new policy. The new policy will now be listed in the main **Virus Scanning Policies** view.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

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 you want to edit.

NOTE: For more information, refer to the [Adding a Virus Scanning Policy](#) section in this chapter.

3. Click **Save Settings** to finalize editing a policy.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

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 you want to enable or disable.


3. Click **Save Settings** to finalize enabling or disabling a policy.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

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 you want to delete.

3. Click **Save Settings** to finalize deleting a policy.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

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**.

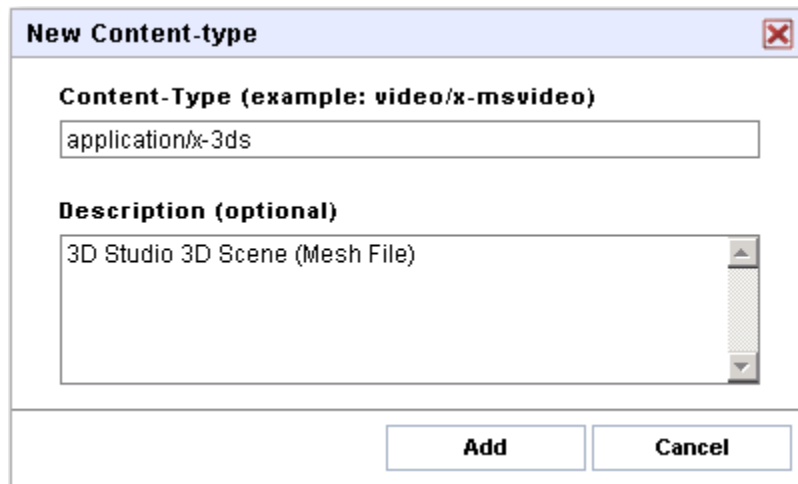
This policy can be edited but it cannot be disabled or deleted. Refer to the [Editing a Virus Scanning Policy](#) section in this chapter for information related to editing virus-scanning policies.

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

NOTE: 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 allows you create new definitions for file types, which are not yet in the predefined list.



The screenshot shows a dialog box titled "New Content-type". It has a close button in the top right corner. The dialog contains two text input fields. The first field is labeled "Content-Type (example: video/x-msvideo)" and contains the text "application/x-3ds". The second field is labeled "Description (optional)" and contains the text "3D Studio 3D Scene (Mesh File)". At the bottom of the dialog are two buttons: "Add" and "Cancel".

Screenshot 56 - 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** to finalize creating a new content-type.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

6.5 Virus & Spyware Protection

The **Virus & Spyware Protection** node allows 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 57 - 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.

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

3. Click **Save Settings** to finalize enabling or disabling a virus-scanning engine.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

6.5.2 Configuring Anti-Virus Updates

The **Anti-Virus Updates** area for each one of the supported anti-virus scanning engines allows 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

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 v1.7 (build 8314.19) (i386) (Sep 29 2008 17:19:14) Signatures:2592126 (2009-03-06 14:42)
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: 2009-03-06 15:42 Updated. Next update check: 2009-03-07 15:42


Screenshot 58 - 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: 6.0.6(10) Signatures:2970120. (2009-03-05 13:50)		
Anti-Virus Engine License Status	Licensed.		
Anti-Virus Updates			
<input checked="" type="checkbox"/> Manage anti-virus updates automatically			
Check for anti-virus updates, and if available install them, every: <input type="text" value="24"/> hours			
<input checked="" type="checkbox"/> Send an email notification to the administrator on successfully updating the anti-virus. <small>NOTE: If an anti-virus update fails, an email notification is always sent to the administrator.</small>			
Anti-virus last updated on: 2009-03-06 10:25 Up-to-date. Next update check: 2009-03-07 10:25			<input type="button" value="Update Now"/>

Screenshot 59 - Norman Anti-Virus view

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

1. Navigate to:

- Option 1: **WebSecurity Edition ► Virus Scanning Policies ► Virus & Spyware Protection** and click the **Edit** icon  next to the anti-virus scanning engine you want to edit.
- Option 2: **WebSecurity Edition ► Virus Scanning Policies ► Virus & Spyware Protection** and select the anti-virus scanning engine from **BitDefender**, **Kaspersky** or **Norman**.

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** to finalize configuration of settings for the selected anti-virus scanning engine to update automatically.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

Configuring Kaspersky Virus-Scanning Engine Options

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

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

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

Anti-virus Engine Status and Version	Active. Version: 4.0.2.29 signatures: 1873923. (2009-03-06 14:29)
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: 2009-03-06 15:29 Updated. Next update check: 2009-03-07 15:29

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 60 - 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** to finalize configuration of settings for the Kaspersky anti-virus scanning engine.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

6.6 Anti-Phishing Engine

The **Anti-Phishing Engine** node allows 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.**

Anti-Phishing Engine Save Settings Cancel

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

General **Notifications**

Block access to phishing sites.

Anti-Phishing Engine Status and Version	Active. Version: 2009-03-06 10:22.
Anti-Phishing Engine License Status	Licensed .

Anti-Phishing Updates

Manage anti-phishing updates automatically

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

Send an email notification to the administrator on successfully updating the anti-phishing.

NOTE: If an anti-phishing update fails, an email notification is always sent to the administrator.

Anti-phishing last updated on: 2009-03-06 10:22 Updated. Next update: 2009-03-07 10:22

Screenshot 61 - 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.

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

4. Click **Save Settings** to finalize enabling or disabling the anti-phishing engine.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

6.6.2 Configuring Anti-Phishing database updates

The **Anti-Phishing Updates** area allows 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. Click the **General** tab.
3. Check the **Manage anti-phishing updates automatically** and update the time period within the **hours** field.
4. Select the **Send an email notification to the administrator on successfully updating the anti-phishing** checkbox if required.
5. Click **Save Settings** to finalize configuration of settings for the anti-phishing engine to update automatically.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

6.6.3 Configuring phishing notifications

The Notifications tab in **Anti-Phishing Engine** node allows 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**.

The screenshot shows the 'Anti-Phishing Engine' configuration window with the 'Notifications' tab selected. The window title is 'Anti-Phishing Engine' and it has 'Save Settings' and 'Cancel' buttons. Below the title bar, there is a description: 'Use this page to configure the anti-phishing engine to protect network users from phishing sites.' The 'Notifications' tab is active, and the 'General' tab is also visible. The main content area contains the following elements:

- A checked checkbox labeled 'Notify the following administrators when the site accessed is a known phishing site.' Below this is a text input field for 'Email Address' with a dropdown arrow and an 'Add' button.
- A table listing email addresses: 'JohnDoe@yourdomain.com' and 'PaulSmith@MyDomain.com', each with a red trash icon to its right.
- A section titled 'Send the following notification to the administrators' with a text area containing the message: 'GFI WebMonitor blocked access to a known phishing site.'
- A checked checkbox labeled 'Notify the user accessing the site if the site accessed is a known phishing site.' Below this is a note: 'NOTE: The notification is sent only if the user performing the download is authenticated.'
- A section titled 'Send the following notification to the user accessing the site' with a text area containing the message: 'GFI WebMonitor protected you from accessing a known phishing site.' Below this is a paragraph of explanatory text: 'A phishing site generally looks like the site of a legitimate business, for example, a financial institution. This tricks many people into disclosing financial and personal information, such as credit card information. The person(s) behind the phishing site can then use this information to steal money from you.'

Screenshot 62 - Anti-Phishing Engine: Notifications tab

2. (Optional) Select the **Notifications** tab and select the **Notify the following administrators when the site accessed is a known phishing site** checkbox to enable notification and define the administrator's notification email address and provide the body text of the notification email.
3. (Optional) Select the **Notify the user accessing the site if the site accessed is a known phishing site** checkbox to enable notification and provide the body text of the notification email.
4. Click **Save Settings** to finalize configuring phishing notifications.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

7 Configuring GFI WebMonitor

7.1 Introduction

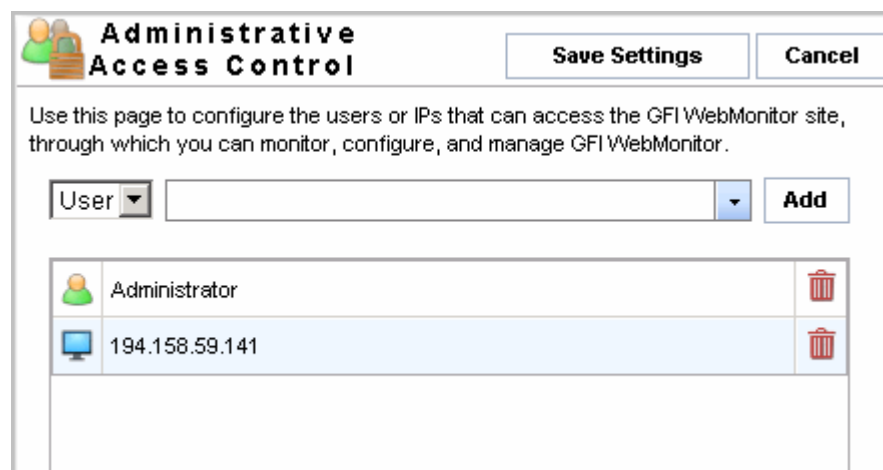
The **Configuration** node and its sub-nodes enable you to configure a default set of parameters used by the WebFilter and WebSecurity editions. The configuration parameters include:





- **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.
- **Proxy settings:** Configure GFI WebMonitor proxy settings
- **Reporting:** Configure the database settings for reporting.

7.2 Administrative Access Control

The **Administrative Access Control** node allows you to list the user(s) and IP(s), which are allowed to access the GFI WebMonitor application (i.e. 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



Administrative Access Control		Save Settings	Cancel
Use this page to configure the users or IPs that can access the GFI WebMonitor site, through which you can monitor, configure, and manage GFI WebMonitor.			
User	<input type="text"/>	Add	
 Administrator			
 194.158.59.141			

Screenshot 63 - 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(s)** and/or **IP(s)**, whom are allowed to access the GFI WebMonitor application from their machine and click, **Add**. Repeat for all the required user(s), group(s) and/or IP(s).


NOTE: When adding a user, specify the username in the format DOMAIN\user.

3. Click **Save Settings** to finalize adding users and/or IP addresses to the access permissions list.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

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 you want to delete.
3. Click **Save Settings** to finalize deleting users/IP addresses.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

7.3 Notifications

The **Notifications** node allows 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.

7.3.1 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** to finalize configuring the sender.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

7.3.2 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
GFIWebMonitor@mydomain.com

SMTP Server **SMTP Port**
192.168.1.64 25

Send administrative emails to the following recipients

Email Address
[Field with dropdown arrow] Add

@	administrator@mydomain.com	
@	engineer@mydomain.com	

Screenshot 64 - 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** to finalize adding recipients.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

7.3.3 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 you want to delete.
3. Click **Save Settings** to finalize deleting recipients.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

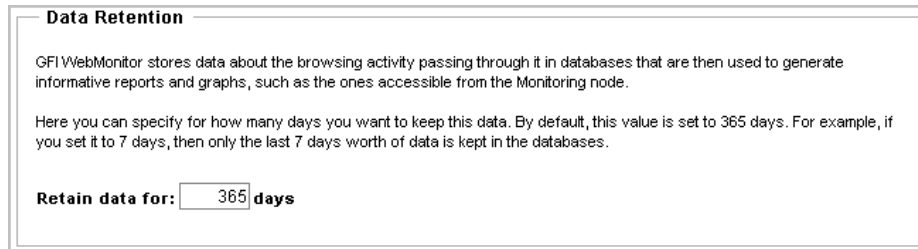
7.4 General Settings

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

- The number of days to keep browsing related data in the database
- The number of hours to keep downloaded files in the cache
- The number of hours a site is kept in the temporary whitelist after it has been approved from the quarantine
- The language in which messages are displayed on the user's machine.

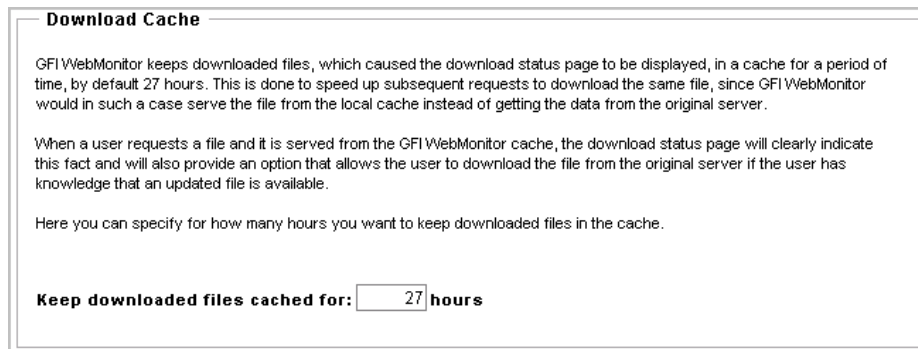
To configure general settings for GFI WebMonitor:

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



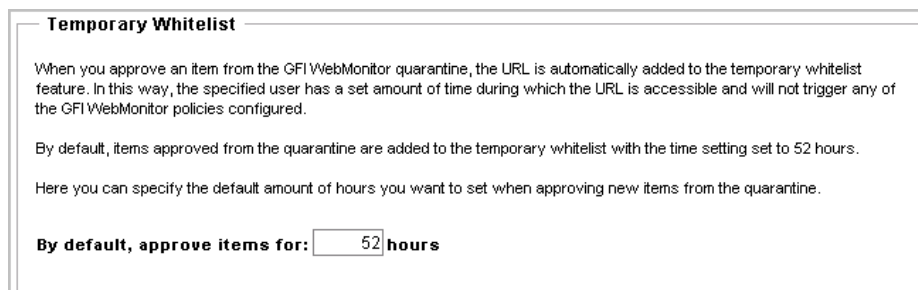
Screenshot 65 - Configuration: General Settings view - Data Retention

2. In the **Data Retention** area, specify for how long (in days) browsing activity data will be kept in the GFI WebMonitor databases. This data is used for monitoring and reporting.



Screenshot 66 - Configuration: General Settings view - Download Cache

3. In the **Download Cache** area, specify 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.



Screenshot 67 - Configuration: General Settings view - Temporary Whitelist

4. In the **Temporary Whitelist** area, specify for how long (in hours) items approved from the quarantine will be kept in the Temporary Whitelist. This is the amount of time available to the user, during which the approved URL is accessible.

NOTE: To disable the Temporary Whitelist set the value to zero hours.

Statistics: Records per Page

GFI WebMonitor provides statistical reports located under the Monitoring node. The time taken for the retrieval of records is proportional to the amount of records displayed per page.

Here you can specify the number of records to be displayed per page.

Display: records per page

NOTE: The minimum value is 100 and the maximum value is 2000 records per page.

Screenshot 68 - Configuration: General Settings view – Statistics: Records per Page

5. In the **Statistics: Records per Page** area, specify the number of records to be displayed per page (default 500 records per page) for every report located under the Monitoring node.

NOTE: This setting does not apply for the Top Categories report.

Language

Please select the language in which GFI WebMonitor displays messages in the client's internet browser.

NOTE: In order for a language change to take effect, the GFI Proxy service must be restarted.

Screenshot 69 - Configuration: General Settings view - Language

6. In the **Language** area, select the language from drop-down list, in which GFI WebMonitor displays messages on the user's machines. Messages from GFI WebMonitor include:

- Download status windows
- Blocking Notifications

7. Click **Save Settings** to finalize configuring general settings for GFI WebMonitor.


NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

7.5 Proxy Settings

The **Proxy Settings** node allows you to configure several proxy settings. The settings include:

- Network Configuration
- Authentication Method
- Chained Proxy

NOTE: This node is only available in GFI WebMonitor Standalone Proxy version.

 **Proxy Settings**

Use this page to specify settings for the proxy and authentication

Tips & Solutions

For important tips and solutions related to common environments and browsers when deploying the GFI WebMonitor proxy please visit the following knowledge base article:

<http://kbase.gfi.com/showarticle.asp?id=KBID001808>

Network Configuration

Configure the network interface and port on which the proxy listens to incoming connections.

Listen on all network interfaces
 Use WPAD for network clients

- Publish the IP of the GFI WebMonitor proxy in WPAD
- Publish the host name of the GFI WebMonitor proxy in WPAD

NOTE: Proxy will always listen for web connections from this computer (127.0.0.1:8080)

Authentication method

Select proxy server authentication method.

No authentication
 Basic authentication
 Integrated authentication

[Click here for more information](#)

Chained Proxy

WebMonitor Proxy will route the web traffic to the following proxy:

Address: Port:

Use the following user credentials as an alternative to the default proxy authentication credentials.
(Leave blank to disable alternative authentication)

Username: Password:

[Click here for more information](#)

Screenshot 70 - Configuration: Proxy Settings view

7.5.1 Configuring Network Configuration

The **Network Configuration** area allows you to configure GFI WebMonitor to listen for incoming connections on a specific network card. The Network Configuration drop-down list contains a list of network cards installed on GFI WebMonitor machine.

To configure on which network interface GFI WebMonitor will listen to incoming connections:

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

Network Configuration

Configure the network interface and port on which the proxy listens to incoming connections.

192.168.5.6

Listen on all network interfaces

Use WPAD for network clients

Publish the IP of the GFI WebMonitor proxy in WPAD

Publish the host name of the GFI WebMonitor proxy in WPAD

NOTE: Proxy will always listen for web connections from this computer (127.0.0.1:8080)

Screenshot 71 - Configuration: Proxy Settings view - Network Configuration

2. Select the IP address of the network card (through which the proxy listens to incoming connections) from the drop-down list, and key in the listening port (default 8080).
3. Select the **Use WPAD for network clients** to allow client machines to detect the server as the default proxy.
4. Select:
 - Option 1: **Publish the IP of the GFI WebMonitor proxy in WPAD** checkbox to include the GFI WebMonitor IP address in the WPAD.dat file.
 - Option 2: **Publish the host name of the GFI WebMonitor proxy in WPAD** checkbox to include the GFI WebMonitor host name in the WPAD.dat file.
5. Click **Save Settings** to finalize configuring on which network interface GFI WebMonitor will listen to incoming connections.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

NOTE: Select the **Listen on all network interfaces** checkbox if the GFI WebMonitor server is required to listen to incoming connections on multiple network cards.

7.5.2 Configuring Authentication Method

The **Authentication Method** area allows you to configure the authentication method used by the proxy. This determines how client machines are validated when accessing the Internet.

Authentication method

Select proxy server authentication method.

No authentication

Basic authentication

Integrated authentication

[Click here for more information](#)

Screenshot 72 - Configuration: Proxy Settings view - Authentication method

No authentication

Select this checkbox if proxy authentication is not required. Thus, the user is not required to key in a valid username and password when

launching a new Internet session. When launched, the Internet browser will not prompt the user to provide valid login credentials.

Basic authentication

Select this checkbox if the user is required to key in a valid username and password when launching a new Internet session. When launched, the Internet browser will prompt the user to provide valid login credentials.

Integrated authentication

Select this checkbox if proxy authentication is required. This is done using the client machines' access control service. Users will not be required to key in login credentials to access the Internet. (Recommended)

The **Integrated authentication** option is disabled on machines where **Local users are authenticated as guest** (This policy is enabled by default on a Microsoft Windows XP Pro machine which has never been joined to a Domain Controller). Network access method can be configured:

- Manually on each machine or,
- Using Active Directory GPO.

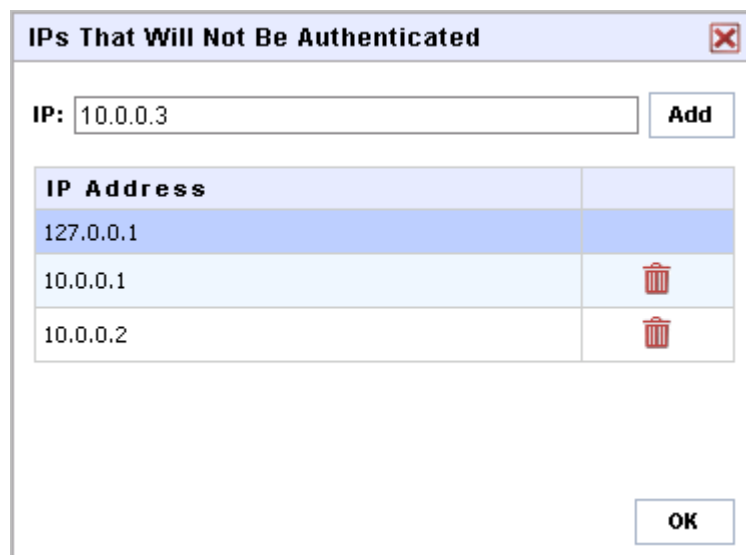
For more information, refer to the [Configuring Network Access policy](#) section in the [Miscellaneous](#) chapter.

Exception List

The **Set Exception List** button allows you to specify the IP addresses that GFI WebMonitor will exempt from proxy authentication.

To add IP addresses:

1. Click the **Set Exception List** button.



Screenshot 73 - Exception list dialog

2. In the **IP** field, specify the IP that is to be excluded and click **Add**. Repeat for all the required IP addresses.
3. Click **OK** to exit the dialog.
4. Click **Save Settings** to finalize adding IP addresses.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

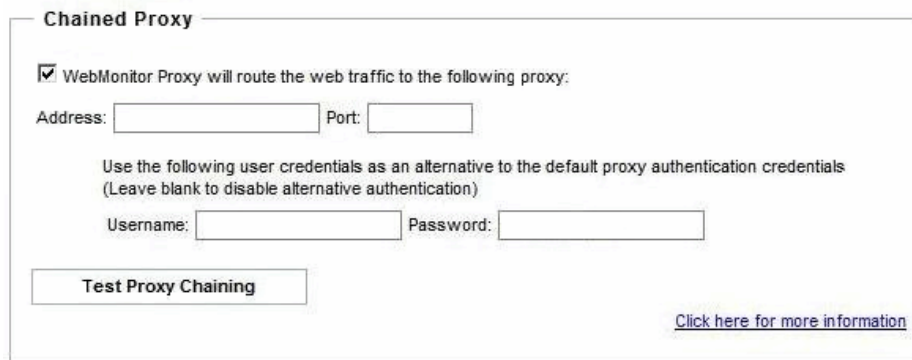
7.5.3 Configuring Chained Proxy

The **Chained Proxy** area allows you to configure the forwarding of HTTP traffic received by the GFI WebMonitor machine to another proxy.

NOTE: Client machines have to be configured to forward HTTP traffic received by them to the GFI WebMonitor machine.

To configure GFI WebMonitor to forward HTTP traffic to a proxy server:

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



Screenshot 74 - Configuration: Proxy Settings view - Chained Proxy

2. Select the **WebMonitor Proxy will route the web traffic to the following proxy:** checkbox.

3. Key in the proxy server IP address in the **Address** text box and key in the chained proxy's port (default 8080) in the **Port** text box.

4. If proxy authentication requires alternate credentials, key in the required credentials in the **Username** and **Password** fields.

NOTE: If no credentials are keyed in, the default user credentials are used.

5. (Optional) Click the **Test Proxy Chaining** button to test the connection between the GFI WebMonitor machine and the proxy server.

6. Click **Save Settings** to finalize configuring GFI WebMonitor to forward HTTP traffic to a proxy server.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

7.6 Reporting

The **Reporting** node allows 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:

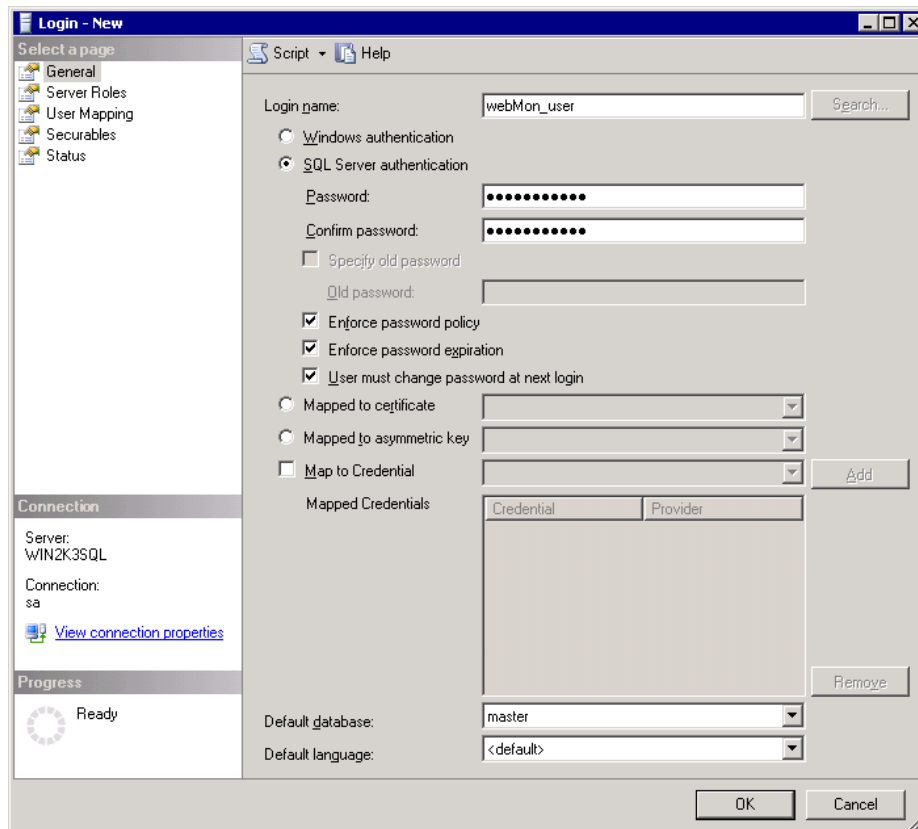
- Reporting requirements
- How to enable or disable information gathering
- Configuring reporting options.

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.

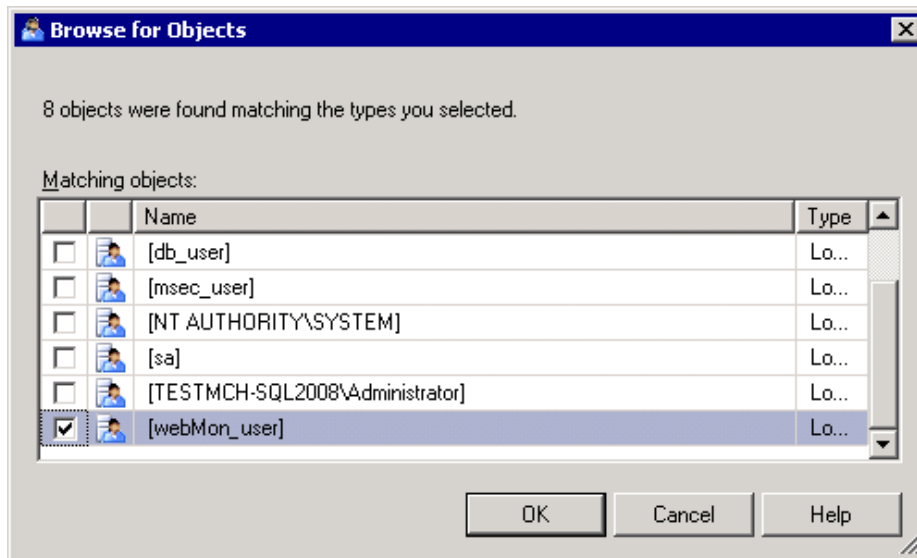
Creating a new database in Microsoft SQL Server 2008

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 75 - 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 76 - 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.

NOTE: 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 Enable 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: [Dropdown]

User: webMon_user

Password: [Masked]

Database: [Dropdown] Get Database List

Reporting Data

Status:

GFI WebMonitor automatically transfers the data logged during the day to the Microsoft SQL Server backend database you configured above. This is done daily at midnight.

If you want to transfer all the past data right now without waiting for midnight, you can click the Update Reporting Data Now button below.

This will save your current settings and transfer all the data logged so far into the Microsoft SQL Server backend database.

Update Reporting Data Now

Screenshot 77 - 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.

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

4. Click **Save Settings** to finalize enabling information gathering for reporting purposes.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

NOTE: 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** to finalize disabling information gathering for reporting purposes.

NOTE: Failing to click **Save Settings** means that you will lose settings as soon as you leave the view to move to another section in GFI WebMonitor.

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.

NOTE: 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.

8 Quarantine

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 allow 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

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, quarantined 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 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:

- 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.

 **Today**

Use this page to review downloads that have been quarantined today.

<input type="checkbox"/>	Quarantined On	User / IP	Download URL	Quarantine Reason
<input type="checkbox"/>	3/6/2009 4:16:52 PM	JohnDoe	http://intl.video.msn.com/s/us/i/im.png	Download control rule blocked Html payload.
<input type="checkbox"/>	3/6/2009 1:58:17 PM	192.168.5.64	http://207.46.110.22/gateway/gateway.dll?Action=poll&SessionID=494951045.1378263819	Download control rule blocked Html payload.

Displaying page 1 of 1 | View page

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:


- Today
- Yesterday
- This Week
- All Items

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:

- **Quarantined On** - the date and time the item was quarantined upon violation of policy
- **User/IP** - the user/IP that is being monitored and 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

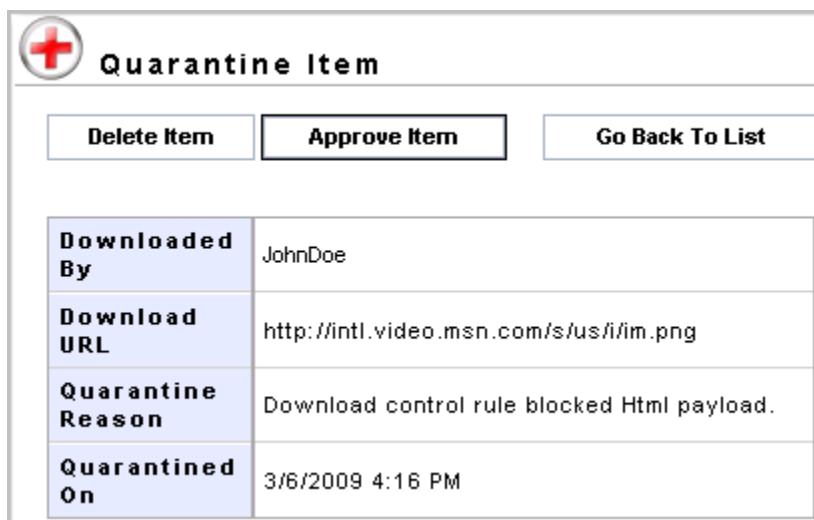
The lists are sorted by **Quarantined On** in descending order.

8.3 Approving quarantined items

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


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.



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.

NOTE: For more information, refer to the [Allowing and blocking users, IP addresses and sites](#) chapter in this manual.

NOTE: 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.

NOTE: 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 allow you to delete any of the entries of the quarantined items. Thus, users are not allowed to access 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 Miscellaneous

9.1 Introduction

The miscellaneous chapter gathers all the other information that falls outside the initial configuration of GFI WebMonitor.

9.2 Configuring Network Access policy

In the **Configuration ► Proxy Settings** area, the **Integrated authentication** option is disabled on GFI WebMonitor machines where the Network access setting is set to **Guest only - local users authenticate as Guest**. On a Microsoft Windows XP Pro machine that has never been joined to a Domain Controller, this setting is set by default.

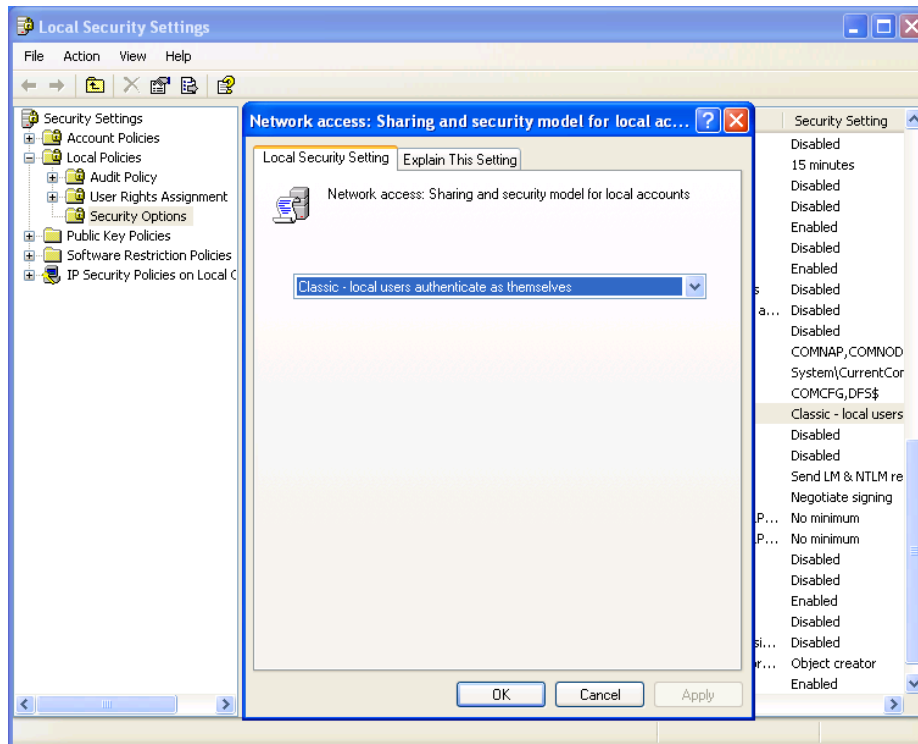
The Network access setting can be configured on each GFI WebMonitor machine:

- Manually or,
- Using Active Directory GPO.

Configuring network access manually

To configure **Network access** setting on a GFI WebMonitor machine manually:

1. Navigate to **Start ► Control Panel ► Administrative Tools ► Local Security Policy**.
2. Expand **Security Settings ► Local Policies ► Security Options**.
3. Right-click **Network access: Sharing and security model for local accounts** from the right panel and click **Properties**.



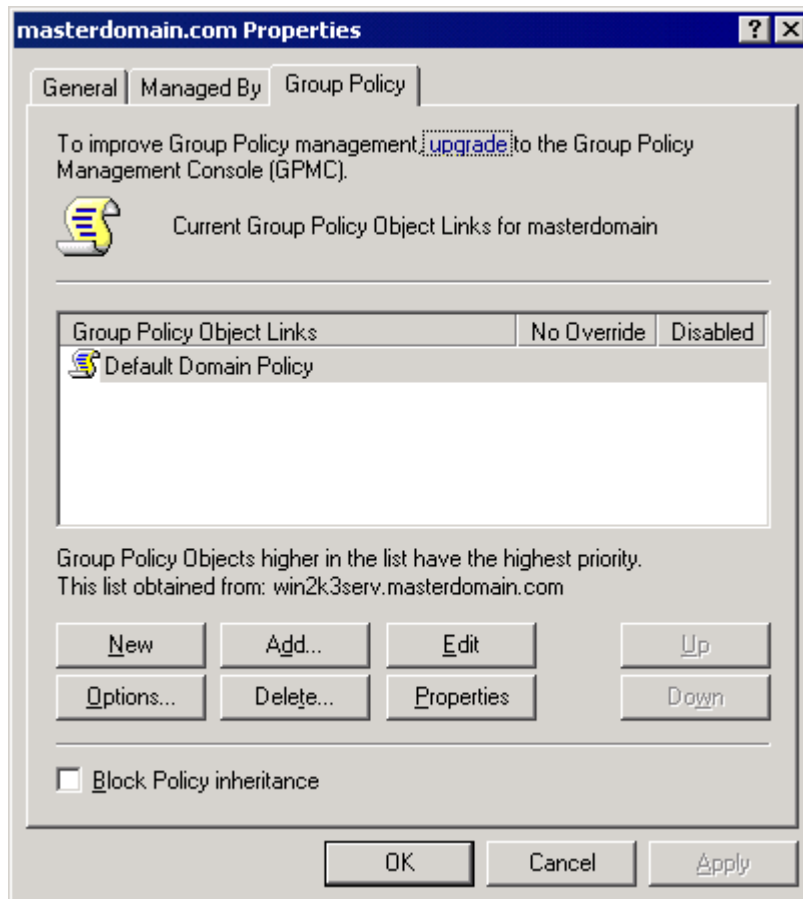
Screenshot 80 - Microsoft Windows XP: Local Security Settings tab

4. Select the **Local Security Setting** tab.
5. Select **Classic - local users authenticate as themselves** from the Network access drop-down list.
6. Click **Apply** and **OK**.
7. Close **Local Security Settings** dialog.
8. Close all open windows.

Configuring network access using GPO in Microsoft Windows Server 2003

To configure **Network access** setting on GFI WebMonitor machines through Microsoft Windows Server 2003 GPO:

1. Navigate to **Start ► Programs ► Administrative Tools ► Active Directory Users and Computers** on the DNS server.
2. Right-click the domain node and click **Properties**.



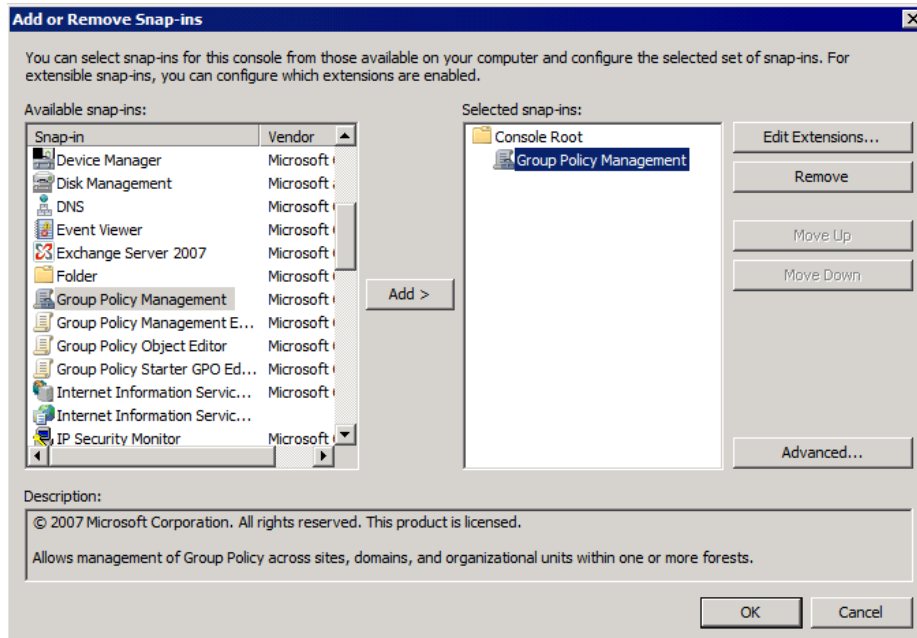
Screenshot 81 - Active Directory GPO dialog

3. Select **Group Policy** tab in the **Domain Properties** dialog.
4. Select **Default Domain Policy** from the list and click **Edit**.
5. Expand **Computer Configuration** ► **Windows Settings** ► **Security Settings** ► **Local Policies** and click **Security Options**.
6. Right-click **Network access: Sharing and security model for local accounts** from the right panel and click **Properties**.
7. In the **Security Policy Setting** tab, check **Define this policy setting** checkbox.
8. Select **Classic - local users authenticate as themselves** from the Network access drop-down list.
9. Click **Apply** and **OK**.
10. Close all open windows.

Configuring network access using GPO in Microsoft Windows Server 2008

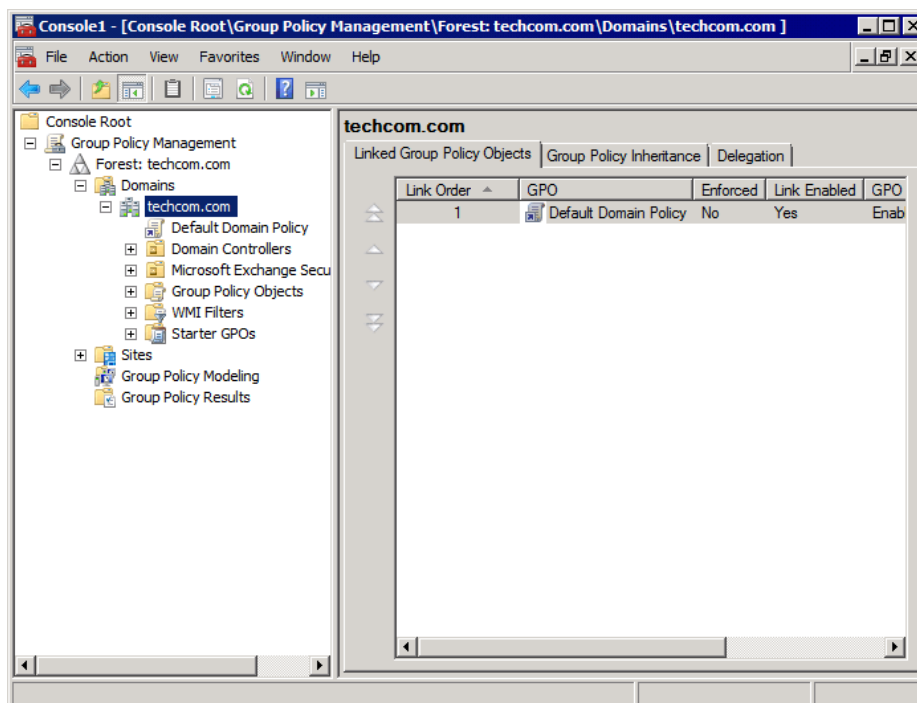
To configure **Network access** setting on GFI WebMonitor machines through Microsoft Windows Server 2008 GPO:

1. In the command prompt key in **mmc.exe** and press **Enter**.
2. In the **Console Root** window navigate to **File** ► **Add/Remove Snap-in...** to open the **Add or Remove Snap-ins** window.



Screenshot 82 - Add/Remove Snap-ins window

3. Select **Group Policy Management** from the **Available snap-ins** list, and click **Add**.
4. Click **OK**.



Screenshot 83 - Console Root domain window

5. Expand **Group Policy Management** ► **Forest** ► **Domains** and **Domain**.
6. Right-click **Default Domain Policy** and click **Edit**. This opens the **Group Policy Management Editor**.
7. Expand **Computer Configuration** ► **Policies** ► **Windows Settings** ► **Security Settings** ► **Local Policies** and click **Security Options**.
8. Right-click **Network access: Sharing and security model for local accounts** from the right panel and click **Properties**.

9. In the **Security Policy Setting** tab, check **Define this policy setting** checkbox.
10. Select **Classic - local users authenticate as themselves** from the Network access drop-down list.
11. Click **Apply** and **OK**.
12. Close **Group Policy Management Editor** dialog and save the management console created.

This information is also available in KBase article:

<http://kbase.gfi.com/showarticle.asp?id=KBID003666>

10 Troubleshooting

10.1 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

10.2 Common Issues

Issue encountered	Solution
Users are not able to browse and/or download from the Internet after installing GFI WebMonitor as a standalone proxy version.	After the installation, GFI WebMonitor proxy machine has to be configured to listen for incoming connections. For more information, refer to the Proxy Settings chapter in this manual. Next, Internet browsers on client machines have to be configured to use the GFI WebMonitor proxy machine as the default proxy. In the event that the users are still not able to browse and/or download from the Internet, add an exception rule in the firewall on the GFI WebMonitor proxy machine to allow incoming TCP traffic on port 8080.
Client browsers are still retrieving old proxy Internet settings although the browsers are configured to automatically detect settings.	Internet explorer may not refresh cached Internet settings so client browsers will retrieve old Internet settings. Refreshing settings is a manual process on each client browser. For more information, refer to the Refresh cached Internet Explorer settings section within the Miscellaneous chapter in GFI WebMonitor Getting Started Guide . Or visit: http://technet.microsoft.com/en-us/library/cc302643.aspx
Users are still required to authenticate themselves manually when browsing, even when Integrated authentication is used.	Integrated authentication will fail when GFI WebMonitor is installed on a Microsoft Windows XP Pro machine that has never been joined to a Domain Controller and where the Network access setting is set to Guest only - local users authenticate as Guest . For more information, refer to the Configuring Network Access policy section in the Miscellaneous chapter.
Users using Mozilla Firefox browsers are repeatedly asked to key in credentials after installing GFI WebMonitor as a standalone proxy version.	The server and the client machine will use NTLMv2 for authentication when: <ul style="list-style-type: none">• GFI WebMonitor is installed on Microsoft Windows Server 2008 and LAN Manager authentication security policy is defined as Send NTLMv2 response only and <ul style="list-style-type: none">• The client machine LAN Manager is not defined (this is the default setting in Microsoft Windows 7) NTLMv2 is not supported in Mozilla Firefox and the user's browser will repeatedly ask for credentials.

To solve this issue do one of the following :

1. Navigate to **Configuration ► Proxy Settings**.
2. In the **Network Configuration** area select the **Use WPAD for network clients** checkbox.
3. Select **Publish the host name of the GFI WebMonitor proxy in WPAD**.

Or change authentication mechanism on either of the following:

On GFI WebMonitor server (Microsoft Windows Server 2008):

1. Navigate to **Start ► Administrative Tools ► Local Security Policy**.
2. Expand **Local Policies ► Security Options**.
3. Right-click **Network Security: LAN Manager authentication level** from the right panel and click **Properties**.
4. Select **Local Security Setting** tab in the **Network Security: LAN Manager authentication level Properties** dialog.
5. Select **Send LM & NTLM - use NTLMv2 session security if negotiated** from the Network security drop-down list.
6. Click **Apply** and **OK**.
7. Close **Local Security Policy** dialog.
8. Close all open windows.

Client machines (Microsoft Windows 7) using Active Directory GPO:

1. Navigate to **Start ► Control Panel ► System and Security ► Administrative Tools ► Local Security Policy**.
2. Expand **Local Policies ► Security Options**.
3. Right-click **Network Security: LAN Manager authentication level** from the right panel and click **Properties**.
4. Select **Local Security Setting** tab in the **Network Security: LAN Manager authentication level Properties** dialog.
5. Select **Send LM & NTLM - use NTLMv2 session security if negotiated** from the Network security drop-down list.
6. Click **Apply** and **OK**.
7. Close **Local Security Policy** dialog.
8. Close all open windows.

For more information visit:

<http://kbase.gfi.com/showarticle.asp?id=KBID001782>

10.3 Knowledge Base

GFI maintains a Knowledge Base, which includes answers to the most common problems. If you have a problem, please consult the Knowledge Base first. The Knowledge Base always has the most up-to-date listing of technical support questions and patches. To access the Knowledge Base, visit <http://kbase.gfi.com/>.

10.4 Web Forum

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

10.5 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.

- **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 please visit <http://www.gfi.com/company/contact.htm>.

NOTE: Before you contact our Technical Support team, please 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.

10.6 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>

11 Glossary

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.
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.
Dashboard	Enables the user to obtain graphical and statistical information related to GFI WebMonitor operations.
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 (trojans, etc.) or forgotten downloads initiated by users.
HTTP	See Hypertext Transfer Protocol.
HyperText Transfer Protocol	A protocol used to transfer hypertext data between servers and Internet browsers.
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.
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.
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.
MSN	See Microsoft Windows Live Messenger
Malware	Short for malicious software. Unwanted software designed to infect a computer such as a virus or a trojan.
Mozilla Firefox	Mozilla Firefox is an open source Internet browser.
NTLM	See NT LAN Manager.
NT LAN Manager	A Microsoft network authentication protocol.
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.
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.
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 retrieve automatically 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	91
Active Connections report	9
Active Directory GPO	70, 81, 87
Activity Log report	23
AD (<i>Active Directory</i>).....	79, 82, 91
Administrative Access Control	
add user and/or IP.....	63
delete user and/or IP.....	64
Administrative Access Control node	63
All Items list.....	77
Anti-Phishing Engine	
enable/disable engine	60
Notifications tab.....	62
Anti-Phishing Engine node.....	60
Anti-Phishing hyperlinks.....	4
Anti-Phishing Updates area	61
anti-virus	4, 91
anti-virus engines	
BitDefender	59
enable/disable engine	58
Kaspersky	59
Norman	59
Anti-Virus Updates area	58
Authentication Method area	69
automatic updates.....	27
GFI WebMonitor.....	27
Microsoft websites.....	27
AV Scanned Downloads	4

B

Bandwidth	91
Bandwidth Consumption reports	14
Bandwidth Usage Trends chart.....	6
Basic authentication	70

Blacklist	91
add item.....	30
delete item.....	31
Blacklist node	30
Build Notifications.....	89

C

Chained Proxy.....	91
Chained Proxy area.....	71
Charts	
Bandwidth Usage Trends chart	6
Hits Over Time chart.....	5
Show Hits Over Time Charts.....	25
Show IM Messages Over Time Chart.....	25
Show Traffic Over Time Chart	25
Top Blocked Categories (Hits) chart	7
Top Categories (Bandwidth) chart	6
Top Categories (Sites) chart.....	6
WebSecurity/WebFilter status and usage chart.....	5
Check URL Category area	42
Common Issues	87
Configuration node.....	63
Console	91
Current Active Connections hyperlink.....	4
Current items in Quarantine hyperlink.....	4

D

Dashboard.....	91
Dashboard node.....	3, 4
Data Retention area	66
Download & IM hyperlinks.....	5
Download Cache area.....	66
Download Control Policies node.....	43

Download Control Policies tab	78
Download Control Policy	
add policy	43
default policy	47
delete policy	47
edit policy	46
enable/disable policy	47
New Content-type dialog	47
Download Control tab.....	45

E

Exception List.....	70
Exceptions tab.....	36

F

FTP (<i>File Transfer Protocol</i>).....	91
--	----

G

General Settings	
Data Retention	66
Download Cache	66
Language	67
Statistics - Records per Page.....	67
Temporary Whitelist	66
General Settings node	65
Getting Started Guide	1
Google Chrome.....	91
GPO (<i>Group Policy Objects</i>)	91

H

hidden downloads	12, 91
Hidden Downloads report.....	10
Hits Over Time chart	5
HTTP (<i>HyperText Transfer Protocol</i>).....	6, 7, 91
HTTP traffic.....	71

I

IM (Instant Messaging) Control	
Policies node.....	48
IM Control Policy	
add policy	48
default policy	52
delete policy	52
edit policy	51
enable/disable policy	52
IM Control tab.....	49

Integrated authentication	70, 81, 87
interrupted / forgotten downloads	10

K

Knowledge Base	88
----------------------	----

L

LAN (<i>Local Area Network</i>).....	92
Language area	67
Last Blocked Requests list	7
Last Blocked Security Threats list	7
LDAP (<i>Lightweight Directory Access Protocol</i>)	92

M

malicious downloads	10
Malware.....	92
Microsoft Forefront TMG (<i>Microsoft Forefront Threat Management Gateway</i>)	91
Microsoft Internet Explorer	91
Microsoft ISA Server (<i>Microsoft Internet Security and Acceleration Server</i>).....	92
Microsoft SQL Server	92
Microsoft SQL Server 2008	72
Microsoft Windows Live Messenger.....	48, 92
Monitoring node.....	9
Mozilla Firefox	87, 92
MSN	48, 92

N

network access	
manual configuration	81
Microsoft Windows Server 2003 GPO configuration	82
Microsoft Windows Server 2008 GPO configuration	83
Network Configuration area.....	68
New Content-type dialog	
Download Control Policy	47
Virus Scanning Policy	57
No authentication	69
Nodes	

Blacklist.....	30
Configuration.....	63
Dashboard.....	3
Monitoring.....	9
Quarantine.....	77
WebFilter Edition.....	33
WebSecurity Edition.....	43
Whitelist.....	27
Notifications	
add recipient.....	65
configure sender.....	64
delete recipient.....	65
Notifications node.....	64
NTLM (<i>NT LAN Manager</i>).....	92
O	
online lookups.....	41
Override Rules area.....	39
P	
Past Connections report.....	10
Permanent Whitelist	
add item.....	28
delete item.....	28
preconfigured sites.....	27
Phishing.....	92
Policies	
Download Control Policies.....	43
IM Control Policies.....	48
Virus Scanning Policies.....	52
Web Filtering Policies.....	33
Port Blocking.....	92
Proxy Server.....	92
Proxy Settings	
Authentication Method.....	69
Chained Proxy.....	71
Network Configuration.....	68
Proxy Settings node.....	67
Q	
Quarantine.....	92

approve item.....	79
delete item.....	79
view item.....	78
Quarantine list	
All Items.....	77
This Week.....	77
Today.....	77
Yesterday.....	77
Quarantine node.....	77

R

Reporting	
disable reporting.....	74
enable reporting.....	73
Reporting node.....	71
ReportPack.....	71
Reports	
Active Connections report.....	9
Activity Log report.....	23
Bandwidth Consumption reports.....	14
Hidden Downloads report.....	10
Past Connections report.....	10
Search.....	12
Sites History reports.....	17
Users History reports.....	18

S

Search node.....	12
Settings	
Administrative Access Control node.....	63
Anti-Phishing Engine node.....	60
General Settings node.....	65
Notifications node.....	64
Proxy Settings node.....	67
Reporting node.....	71
Virus & Spyware Protection node.....	57
WebGrade Database node.....	40
Show Hits Over Time Charts.....	25
Show IM Messages Over Time Chart.....	25
Show Traffic Over Time Chart.....	25

Site Access History view	21, 22
Sites History reports	17
snap-ins	83
Spyware	92
Statistics - Records per Page area	67

T

Technical Support	89
Temporary Whitelist	
add item	29
delete item	30
Temporary Whitelist area	66
This Week list	77
Today list	77
Top Blocked Categories (Hits) chart	7
Top Categories (Bandwidth) chart	6
Top Categories (Sites) chart	6
Top Categories report	16
Top Hits Count report, Sites History	17
Top Hits Count report, Users History	19
Top Policy Breakers report	20
Top Sites report	14
Top Surfers report	18
Top Time Consumption report	17
Top Users report	15
Traffic Forwarding	92

U

unattended downloads	10
unwanted downloads	10
Update Reporting Data Now button	75
URL (<i>Uniform Resource Locator</i>)	92
User Agent	92
User History Details view	22
Users History reports	18

V

valid updates	10
View	
Site Access History	21, 22
User History Details	22
Virus	92
Virus & Spyware Protection node	57

Virus Scanning Policies node	52
Virus Scanning Policies tab	78
Virus Scanning Policy	
add policy	53
default policy	56
delete policy	56
edit policy	56
enable/disable policy	56
New Content-type dialog	57
Virus Scanning tab	54

W

WAN (<i>Wide Area Network</i>)	93
Web Filtering hyperlinks	5
Web Filtering Policies node	33
Web Filtering Policies tab	78
Web Filtering Policy	
add advanced condition	39
add policy	34
advanced conditions	39
default policy	38
delete advanced condition	40
delete policy	38
edit advanced condition	40
edit policy	38
enable/disable policy	38
Web Filtering tab	35
Web Forum	88
web traffic	92
WebFilter Edition	27, 63, 92
WebFilter Edition node	33
WebGrade Database	33, 92
enable/disable database	41
WebGrade Database node	40
WebGrade Database Updates area	42
WebSecurity Edition	27, 63, 93
WebSecurity Edition node	43
WebSecurity/WebFilter status and usage chart	5
Whitelist	93
Permanent	12, 27
Temporary	27
Whitelist node	27
Whitelist, Permanent	

add item	28
delete item.....	28
preconfigured sites.....	27
Whitelist, Temporary	
add item	29
delete item.....	30
wildcards	31

WPAD (<i>Web Proxy AutoDiscovery protocol</i>)	69, 87, 92
--	------------

Y

Yesterday list.....	77
---------------------	----