Product Manual

# **GF** WebMonitor

# Administration and Configuration Manual





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or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors.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

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

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

Last updated: 12 September 2011 Version number: WEBMON-GSG-EN-2.1.0

# Contents

1	Introd	luction	1
	1.1 1.2 1.3 1.4 1.5	Who is This Manual For? About this Manual Terms Used in This Manual GFI WebMonitor Editions GFI WebMonitor Licensing	1 2 2 3
2	About	t GFI WebMonitor	5
	2.1 2.2	How Does GFI WebMonitor Work? How to Deploy GFI WebMonitor	5 6
3	Instal	ling in Gateway Mode	9
	3.1 3.2 3.3 3.4	Introduction System Requirements Installation Post-installation Actions: Configure Proxy Settings	,.9 9 .10 .13
4	Instal	ling in Simple Proxy Mode	23
	4.1	Introduction	.23
	4.Z	System Requirements	. Z3
	4.3	Post-installation Actions: Configure Proxy Settings	. 27
5	Launo	ching GFI WebMonitor	37
	51	Introduction	37
	5.2	Launching GFI WebMonitor	. 37
	5.3	Navigating the Console	. 37
6	Misce	llaneous	39
	6.1	Introduction	. 39
	6.2	Entering Your License Key After Installation	. 39
	6.3	Enabling WPAD in Proxy Settings	. 39
	6.4	Refreshing Cached Microsoft Internet Explorer Settings	. 40
	0.D	Configuring Pouting and Perote Access	.40 1
	6.7	Configuring Commonly Used Routers	42
	6.8	Disabling Internet Connections Settings on Client Machines	. 58
	6.9	Assigning Log On As A Service Rights	. 62
	6.10	Configuring Network Access Policy	. 67
7	Troub	oleshooting	71
	7.1	Introduction	.71
	7.2	Common Issues	.71
	7.3	Knowledge Base	.72
	7.4	Web Forum	.73
	7.5	Request Technical Support	.73

	7.6	Build Notifications	73
8	Glossa	ary	75
Inde	ex		79

# 1 Introduction

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

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

#### 1.1 Who is This Manual For?

This manual is for system administrators who want to use GFI WebMonitor in standalone proxy mode (for example, in environments where there is no Microsoft ISA Server or Microsoft Forefront TMG).



Figure 1 - Environment: GFI WebMonitor in standalone proxy mode

For environments with Microsoft ISA Server or Microsoft Forefront TMG, a dedicated version of GFI WebMonitor (GFI WebMonitor for ISA/TMG) is available. For more information, refer to: http://www.gfi.com/isa-server-monitoring-security.

#### 1.2 About this Manual

The aim of this manual is to help you install and run GFI WebMonitor on your network with minimum configuration effort. It describes:

- » The various network environments that GFI WebMonitor can support.
- » How to install GFI WebMonitor to monitor your environment.
- » How to get GFI WebMonitor running on default settings.

This manual is structured as follows:

CHAPTER	DESCRIPTION
Chapter 1	Introduction
	Introduces this manual and provides information on GFI WebMonitor editions.
Chapter 2 About GFI WebMonitor	
	Provides a high-level overview of how GFI WebMonitor works and the different installation environments supported.
Chapter 3 Installing in Gateway Mode	
	Provides information on how to install GFI WebMonitor in Gateway mode.
Chapter 4 Installing in Simple Proxy Mode	
	Provides information on how to install GFI WebMonitor in Simple Proxy mode.

CHAPTER	DESCRIPTION	
Chapter 5	Launching GFI WebMonitor	
	Provides a high-level overview of the user console.	
Chapter 6	Miscellaneous	
	Provides information on topics that do not strictly fall within other chapters.	
Chapter 7	Troubleshooting	
	Provides all the necessary information on how to deal with any problems encountered while using GFI WebMonitor. Also provides extensive support information.	
Chapter 8	Glossary	
	Defines technical terms used within GFI WebMonitor.	

#### 1.2.1 Administration and Configuration Manual

Detailed administration and configuration guidelines are provided in the Administration and Configuration Manual that is installed with the product or separately downloadable from the GFI website at http://www.gfi.com/products/gfi-webmonitor/manual.

#### 1.3 Terms Used in This Manual

The following terms are used in this manual:

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

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

#### 1.4 GFI WebMonitor Editions

GFI WebMonitor is available in three editions. Each edition caters for system administrators with different requirements:

- WebFilter Edition: Filters web traffic and website use per user(s), group(s) and/or IP(s) and manages Internet access during specific periods, based on web categories defined within its built-in WebGrade database.
- WebSecurity Edition: Provides a high degree of web security for downloaded web traffic. This is achieved through the built-in download control module and multiple anti-virus and anti-spyware engines.
- » **Unified Protection Edition:** Provides all the features of the WebFilter Edition and the WebSecurity Edition in a single package.

## 1.5 GFI WebMonitor Licensing

For more information about licensing, refer to GFI Software Ltd. website at:

http://www.gfi.com/products/gfi-webmonitor/pricing/licensing

For more information on how GFI WebMonitor counts users for licensing purposes, refer to Knowledge Base article:

http://kbase.gfi.com/showarticle.asp?id=KBID003528.

# 2 About GFI WebMonitor



#### 2.1 How Does GFI WebMonitor Work?

Figure 2 - How does GFI WebMonitor work?

**V** Request initiation: Users request a webpage or a download from the Internet. The incoming traffic generated by the user's request is forwarded to GFI WebMonitor.

**2** Blacklist/Whitelist filtering: The internal GFI WebMonitor blacklist/whitelist filtering mechanism analyzes the user ID, IP address and requested URLs, taking the following actions:

ACTION	DESCRIPTION
Blocks web traffic requests	<ul> <li>by blacklisted users and/or IP addresses, or</li> <li>to access blacklisted URLs</li> </ul>
Automatically allows web traffic requests	» by whitelisted users and/or IP addresses, or
	» to access whitelisted URLs
Forwards web traffic requests (to the WebFilter module)	<ul> <li>by users and/or IP addresses that are neither blacklisted nor whitelisted</li> </ul>
	» to access URLs that are neither blacklisted nor whitelisted.

**WebFilter module:** Analyzes web traffic received from the blacklist/whitelist filtering mechanism against a list of categories stored in GFI WebMonitor's WebGrade database. These categories are used to classify and then filter web pages requested by users.

For more information about these categories, refer to Knowledge Base article: http://kbase.gfi.com/showarticle.asp?id=KBID003165. Web traffic is blocked, allowed or quarantined according to configured policies. Quarantined web traffic can be manually approved or rejected by the administrators according to the user's needs and requirements. Approved quarantined URLs are moved in a temporary whitelist; a mechanism used to approve access to a site for a user or IP address for a temporary period.



The WebFilter module is only available in the WebFilter Edition and the Unified Protection Edition of GFI WebMonitor. In the WebSecurity Edition, web traffic is sent directly from the whitelist/blacklist filtering mechanism to the WebSecurity module.

**WebSecurity module:** Analyzes web traffic through the download control module and scans incoming web traffic for viruses, spyware and other malware.

Infected material is allowed, blocked and quarantined or blocked and deleted according to the configured policies. Web traffic is also scanned for phishing material against a list of phishing sites stored in the updatable database of phishing sites. Web traffic generated from a known phishing element is rejected while approved web material is forwarded to the user.



The WebSecurity module is only available in the WebSecurity Edition and Unified Protection Edition of GFI WebMonitor. In the WebFilter Edition, WebSecurity processing is not performed, and web traffic is forwarded on to the user.

Forwarding of approved web material by GFI WebMonitor to the user depends on the network environment; that is, where GFI WebMonitor is installed.

#### 2.2 How to Deploy GFI WebMonitor

#### 2.2.1 Introduction

GFI WebMonitor deployment depends on the network infrastructure and the network role of the machine where GFI WebMonitor is to be installed. The following diagram is aimed to help you choose the correct GFI WebMonitor installation mode to suit your environment.



Figure 3 - Choosing your environment flow chart

#### 2.2.2 Internet Gateway Environment

Install GFI WebMonitor in Gateway mode when an internet gateway is used by client machines to access the internet. GFI WebMonitor can be installed on the internet gateway machine to filter and process all outgoing/incoming HTTP/HTTPS traffic generated from/to user machines.



Figure 4 - GFI WebMonitor installed on a gateway machine

To install GFI WebMonitor on an Internet gateway, refer to the Installing in Gateway Mode chapter in this manual.

#### 2.2.3 Simple Proxy Environment

Install GFI WebMonitor in Gateway mode when using a router/gateway for port blocking or traffic forwarding.

#### Port Blocking

The router/gateway must be configured to allow both HTTP/HTTPS traffic generated from GFI WebMonitor machine and Non-HTTP/HTTPS traffic generated from client machines. In addition, it must also block HTTP/HTTPS traffic generated from client machines.



Client machines must be configured to use the GFI WebMonitor machine as the default proxy server.



Figure 5 - GFI WebMonitor installed on a proxy machine connected to a router supporting port blocking

# Traffic Forwarding

The router/gateway must be configured to allow outgoing web traffic generated by GFI WebMonitor only. In addition, it must forward client HTTP/HTTPS traffic to GFI WebMonitor.



Figure 6 - GFI WebMonitor installed on a proxy machine connected to a router supporting traffic forwarding

To install GFI WebMonitor on a proxy server, refer to the Installing in Simple Proxy Mode chapter in this manual.

# 3 Installing in Gateway Mode

#### 3.1 Introduction

This chapter provides you with information related to the installation of GFI WebMonitor on a machine configured as an Internet Gateway.

#### 3.2 System Requirements

#### 3.2.1 Software

ТҮРЕ	SOFTWARE REQUIREMENTS	
Supported Operating Systems	» Microsoft Windows Server 2003 (x86)	
	» Microsoft Windows Server 2008 (x86 or x64)	
	» Microsoft Windows Server 2008 R2 (x64)	
	» Microsoft Windows XP SP2	
	» Microsoft Windows Vista	
	» Microsoft Windows 7	
Other required components	» Microsoft Internet Explorer 7 or later	
	» Microsoft.NET Framework 2.0	
	» Microsoft Message Queuing Service (MSMQ)	
	<ul> <li>Routing and Remote Access configuration on Microsoft Windows Server 2003/2008</li> </ul>	
	<ul> <li>Microsoft SQL Server 2000 or later (for reporting purposes)</li> </ul>	

#### 3.2.2 Hardware

Minimum hardware requirements depend on the GFI WebMonitor edition.

EDITION	HARDWARE REQUIREMENTS	
All Editions	» Two Network Interface Cards	
WebFilter Edition	<ul> <li>» Processor: 2.0 GHz</li> <li>» RAM: 1 GB (Recommended 4GB)</li> </ul>	
	<ul> <li>Hard disk: 2 GB of available disk space</li> </ul>	
WebSecurity Edition	» Processor: 2.0 GHz	
	» RAM: 1 GB (Recommended 4GB)	
	» Hard disk: 10 GB of available disk space	
Unified Protection Edition	» Processor: 2.0 GHz	
	» RAM: 2 GB (Recommended 4GB)	
	» Hard disk: 12 GB of available disk space	



Allocation of hard disk space depends on your environment. The size specified in the requirements is the minimum required to install and use GFI WebMonitor. The recommended size is between 150 and 250GB.

#### 3.3 Installation

#### 3.3.1 Pre-requisites

Before installing GFI WebMonitor on an Internet Gateway Server, ensure that:

- 1. Client machines are configured to use the server as the default internet gateway.
- 2. The server's network cards are connected:
- » one to the internal network (LAN)
- » one to the external network (WAN).

3. Start **Routing and Remote Access** service if installing GFI WebMonitor on Microsoft Windows Server 2003 or Microsoft Windows Server 2008. For more information, refer to the Configuring Routing and Remote Access section in this manual.

4. Ensure that the listening port (default 8080) is not blocked by your firewall. For more information on how to enable firewall ports on Microsoft Windows Firewall, refer to http://kbase.gfi.com/showarticle.asp?id=KBID003879

#### 3.3.2 Upgrades

In order to upgrade GFI WebMonitor, obtain the latest version from

http://www.gfi.com/pages/webmon-selection-download.asp. The upgrade procedure is similar to the installation procedure. For more information, refer to the Installation Procedure section in this chapter.



If installing a new version of GFI WebMonitor on a different infrastructure, it is recommended to uninstall the previous version before installing the new one.

#### 3.3.3 Installation Procedure

Run the installer as a user with administrative privileges on the target machine.

1. Double click the GFI WebMonitor executable file.

2. If the current version of Microsoft .NET Framework is not compatible with the required version, a warning dialog will be displayed. Click **OK**. This will stop the installation process. Install the required Microsoft .NET Framework version and start the installation of GFI WebMonitor again.

3. Choose whether you want the installation wizard to search for a newer build of GFI WebMonitor on the GFI website and click **Next**.

4. Read the licensing agreement. To proceed with the installation select I accept the terms in the license agreement and click Next.

🥵 GFI WebMonitor 2011 - InstallShield Wizard 🛛 🛛 🔀			
WebMonitor Configuration - Access Permissions         Specify who will be able to access the GFI WebMonitor Web interface.			
By default only an administrator logged in on this computer will be authorized to access the GFI WebMonitor web interface. GFI WebMonitor can be configured to allow other users/computers to access its web based interface over the network.			
Enter the user name or the computer IP which will be granted access to GFI WebMonitor:			
127.0.0.1;192.168.3.81;192.168.200.7;192.168.3.81			
NOTE: Specify username(s) in the format DOMAIN\username. NOTE: The IP of this computer is already added to the access permission list.			
NOTE: You can specify more than one user/computer. Separate entries with a semicolon (;) eg. 127.0.0.1;COMPANY\user1;COMPANY\user2;172.16.135.16			
InstallShield			
< Back Next > Cancel			

Screenshot 1 - Installation: Access Permissions

5. Key in the user name or the IP address that will be used to access the web interface of GFI WebMonitor and click **Next**.



More than one user or machine can be specified. Separate entries with semicolons ';'

🕏 GFI WebMonitor 2011 - InstallShield Wizar	i 🛛 🔀
<b>Customer Information</b> Please enter your information.	GF
<u>U</u> ser Name: Bob Jones <u>O</u> rganization: myCompany	
License Key: Evaluation InstallShield < Back	Next > Cancel

Screenshot 2 - Installation: Customer Information

6. Key in the **User Name** and **Organization**. If you have a license key, update the **License Key** details and click **Next**.



The license key can be keyed in after installation or expiration of the evaluation period of GFI WebMonitor. For more information, refer to the Entering Your License Key After Installation section in this manual.

🔂 GFI WebMonitor 2011 - InstallShield Wizard 🛛 🔀				
Service Logon	Service Logon Information			
The following lo	The following logon information is used by the WebMonitor Service			
The GFI WebMonitor service needs to run with administrative privileges for proper functionality. Please enter the username and password of an account with administrative privileges. Please make sure that the account is active and does not have the password set to expire. For domains, user names must be in the format of DOMAIN\UserName.				
User Name:	administrator			
Password:	****			
NOTE: The username and password provided must have "Logon As Service" rights. If it doesn't it will be switched ON automatically for the specified account. These credentials will only be used to create and run as new service in the services control panel. InstallShield				
	< Back Next > Cancel			

Screenshot 3 - Installation: Service Logon Information

7. Key in the logon credentials of an account with administrative privileges and click Next.

The user account must have **Log on as a service** rights; otherwise, rights are automatically assigned. For more information, refer to the Assigning Log On As A Service Rights section in this manual.

🕞 GFI WebMonitor 2011 - InstallShield Wizard 🛛 🛛 🔀			
Mail Settings Enter administrator	r email and SMTP mail server settings	GF	
Please enter the details of the SMTP server and email address that are to be used by GFI WebMonitor 2011 for email reporting.			
From:	WebMonitor@127.0.0.1		
To:	Administrator@127.0.0.1		
SMTP Server:	127.0.0.1	Port: 25	
Verify Mail Settings			
	< <u>B</u> ack	Next > Cancel	

Screenshot 4 - Installation: Mail Settings

8. Provide the SMTP mail server details and email address to which administrator notifications will be sent.

Optionally click Verify Mail Settings to send a test email. Click Next.

9. Click Next to install in default location or click Change to change installation path.

10. If the Microsoft Message Queuing Service (MSMQ) is not installed, a message will prompt the user that the installation requirements have not been met. Click **Next** to install the service automatically.

11. Click Install to start the installation, and wait for the installation to complete.

12. Click **Finish** to finalize setup.

13. After the installation, **GFI WebMonitor Configuration Wizard** is launched automatically. This will help you configure the server in gateway mode.

14. In the welcome screen, click Next.

15. Select Gateway mode as your network environment and click Next.

16. In the **Current Gateway Configuration** screen, select the internal network card and click **Next**.

17. Click Finish to apply settings.

#### 3.3.4 Launching GFI WebMonitor

There are 2 options for launching the GFI WebMonitor web console:

- » Option 1: click Start ► Programs ► GFI WebMonitor ► GFI WebMonitor. Further information can be found in the section entitled Launching GFI WebMonitor in this document.
- » **Option 2:** Key in the URL http://monitor.isa in a web browser on the same machine.



If using the GFI WebMonitor through the web browser interface on the same machine, Internet Explorer must be configured to use a proxy server. For more information refer to Microsoft Internet Explorer section in this manual.

To launch GFI WebMonitor installation from machines of users and/or IP addresses that were allowed access to the application during installation:

» Key in the URL http://monitor.isa in a web browser from their machine. The Internet browser must be configured to use specific proxy settings to enable this access.

#### 3.4 Post-installation Actions: Configure Proxy Settings

Configure the user machines to use GFI WebMonitor machine as the default proxy. This can be achieved by:

- » **Option 1:** Configuring the client machines using the Group Policy object (GPO) feature within the Active Directory.
- » **Option 2:** Configuring Internet browsers to use specific proxy settings on each client machine manually.



The client internet browser can be configured to detect the proxy settings automatically. This is possible if WPAD is enabled in GFI WebMonitor proxy settings. For more information, refer to the Enabling WPAD in Proxy Settings section in this manual.

#### 3.4.1 Configuring GFI WebMonitor Machine as the Default Proxy Using GPO in Microsoft Windows Server 2003

To configure the **Proxy Settings** on all client machines to use GFI WebMonitor as a proxy server through Microsoft Windows Server 2003 GPO:

1. Navigate to **Start ► Programs ► Administrative Tools ► Active Directory Users and Computers** on the Domain Controller.

2. Under the domain node, right-click the organizational unit where you wish to apply the group policy and click **Properties**.



masterdomain.com Properties 🛛 🔋 🗙					
General Manage	d By Group Po	licy			
To improve Group Management Cor	p Policy manager hsole (GPMC).	ment <u>upgrade</u> l	to the Group Po	olicy	
	Current Group Policy Object Links for masterdomain				
Group Policy Ol S Default Dom	bject Links nain Policy		No Override	Disabled	
r Group Policy Obje This list obtained	ects higher in the from: win2k3serv	list have the hi /.masterdomain	ighest priority. .com		
New	A <u>d</u> d	<u>E</u> dit		Цр	
Options	Dele <u>t</u> e	<u>P</u> roperties		Do <u>w</u> n	
Block Policy inheritance					
		ОК	Cancel	Apply	

Screenshot 5 - 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**.



Screenshot 6 - GPO Editor window

5. Expand User Configuration ► Windows Settings ► Internet Explorer Maintenance ► Connection and double-click Proxy Settings to open the Proxy Settings dialog.

Prox	y Settings						? ×
Pro	xy Settings						
Ye se	ou can specify eparate entrie	y what proxy servers, if any, you es.	u want y	your user	's to (	o connect to. Use semicolons ( ; ) to	
F	Enable pro:	xy settings					
Г	Proxy Server	′s				Exceptions	- II
		Address of proxy		Port		Do not use proxy server for	
	<u>1</u> . HTTP:	192.168.5.110	:	8080		addresses beginning with:	
	2. Secure:	192.168.5.10	:	8080			
	<u>3</u> , FTP:	192.168.5.110	:	8080			
	<u>4</u> . Gopher:	192.168.5.10	:	8080			
	<u>5</u> . Socks:	192.168.5.10	:	8080			
	Use the	same proxy server for all addres	ses			I Do not use proxy server for local (intranet) addresses.	
				ЭК		Cancel Apply Help	

Screenshot 7 - Proxy Settings dialog

6. Check Enable proxy settings checkbox.

7. Uncheck Use the same proxy server for all addresses checkbox.

8. Key in the proxy server IP address and the port used (Default 8080) in the HTTP and FTP text boxes.

9. Click **OK** to apply changes.

10. Close all open windows.

#### 3.4.2 Configuring GFI WebMonitor Machine as the Default Proxy Using GPO in Microsoft Windows Server 2008

To configure the **Proxy Settings** on all client machines to use GFI WebMonitor as a proxy server through Microsoft Windows Server 2008 GPO:

1. In 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.

			Console Root		Ealt Extensions
Device Manager	Microsoft		Group Policy Mar	agement	
Disk Management	Microsoft				Remove
DNS	Microsoft				
Event Viewer	Microsoft				Move Up
Exchange Server 2007	Microsoft (				( in the set
Folder	Microsoft 🦳				Move Down
Group Policy Management	Microsoft (	Add >			
Group Policy Management E	Microsoft (				
Group Policy Object Editor	Microsoft				
Group Policy Starter GPO Ed	Microsoft				
Internet Information Servic	Microsoft				
Internet Information Servic	_				
IP Security Monitor	Microsoft 🖾				Advanced
					Auvanceu
					Advanced

Screenshot 8 - Add/Remove Snap-ins window

#### 3. Select Group Policy Management from the Available snap-ins list, and click Add.

4. Click OK.

🚟 Console1 - [Console Root\Group Policy	Management\Forest: techcom.com\Domains\techcom.com ]
🚟 File Action View Favorites Window	Help
🗢 🔿 🗡 📊 📋 📖 🧟 📝 🖬	
Console Root	techcom.com
<ul> <li>Koroup Policy Management</li> <li>Korest: techcom.com</li> </ul>	Linked Group Policy Objects Group Policy Inheritance Delegation
🗆 📑 Domains	Link Order 🔺 GPO Enforced Link Enabled GPO
techcom.com     Topfault Domain Policy	🚖 1 🚮 Default Domain Policy No Yes Enab
Denair Controllers	
🕀 💼 Microsoft Exchange Secu	
Group Policy Objects	
H Starter GPOs	¥

Screenshot 9 - Console Root domain window

5. Expand **Group Policy Management** ► **Forest** ► **Domains** and **<domain>**, then select the organizational unit where you wish to apply the group policy.



To apply the group policy to all the computers on the domain, select the domain node directly.

6. Right-click **Default Domain Policy** and click **Edit** to open the **Group Policy Management Editor**.



Screenshot 10 - GPO Editor window

7. Expand User Configuration ► Policies ► Windows Settings ► Internet Explorer Maintenance ► Connection and double-click Proxy Settings to open the Proxy Settings dialog.

Proxy Set	ttings								? ×
Proxy Se	ttings								
You car separat	n specify te entrie able prox	y what proxy servers, if any, you es. Gopher cannot be customized xy settings	u want y I in Inter	our users net Explo	s to c orer 7	:onnect 7.	to. Us	e semicolons (	(; ) to
Proxy	y Server	'S			_	Exce	ptions		
		Address of proxy		Port		Don	iot use	proxy server	for
1. H	ITTP:	192.168.5.110	:	8080		addr	esses	beginning with	1:
2. S	ecure:	192.168.5.10	:	8080					<u>^</u>
3. F	TP:	192.168.5.110	:	8080					
4. G	opher:	192.168.5.10	:	8080					
5. S	ocks:	192.168.5.10	:	8080					×
	Use the	same proxy server for all addres	sses				Do not local (i	t use proxy ser ntranet) addre	esses.
			0	Ж		Cancel		Apply	Help

Screenshot 11 - Proxy Settings dialog

8. Check Enable proxy settings checkbox.

9. Uncheck Use the same proxy server for all addresses checkbox.

10. Key in the proxy server IP address and the port used (Default 8080) in the HTTP and FTP text boxes.

- 11. Click **OK** to apply changes
- 12. Close Proxy Settings dialog.
- 13. Close Group Policy Management Editor dialog and save the management console.



When using Active Directory, the administrator can disable the Internet connection settings tab from the client machines. For more information, refer to the Disabling Internet Connections Settings on Client Machines section in this manual.

#### 3.4.3 Configuring Internet Browsers to Use a Proxy Server

You can also configure each individual user machine manually to set the GFI WebMonitor machine as the default proxy. This section shows how to configure proxy settings in the most commonly used internet browsers.

#### Microsoft Internet Explorer

- 1. Launch Microsoft Internet Explorer.
- 2. From the Tools menu, choose Internet Options and select the Connections tab.
- 3. Click LAN settings button.

Local Area Network (LAN) Settings 🛛 🔹 💽				
Automatic configuration				
Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.				
Automatically detect settings				
Use automatic configuration script				
Address				
Proxy server				
Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).				
Address: myproxy Port: 8080 Advanced				
Bypass proxy server for local addresses				
OK Cancel				

Screenshot 12 - LAN Settings dialog

4. Check Use a proxy server for your LAN checkbox.

5. Key in the proxy server name or IP address of the GFI WebMonitor machine and the port used (Default 8080) in the **Address** and **Port** text boxes.



- 6. Click OK to close LAN Settings dialog.
- 7. Click OK to close Internet Options dialog.

# Mozilla Firefox

1. Launch Mozilla Firefox.

2. Click **Tools** ► **Options** ► **Advanced** tab ► **Network** tab.

Options							×
Main	Tabs	Content	Applications	<b>erivacy</b>	Security	Advanced	
General Conn	Network L	Jpdate Encr	yption				
Confi	gure how Fi e Storage	irefox conne	cts to the Inter	net	_	S <u>e</u> ttings	
Use u	ip to 50 jell me wher	) 🗘 MB of n a website a	space for the c asks to store da	ache ta for offlin	e use	<u>C</u> lear Now E <u>x</u> ceptions	
The f	ollowing we	bsites have	stored data for	offline use:			
						Remove	
				ок	Cancel	Help	

Screenshot 13 - Mozilla Firefox: Options dialog

3. Click Settings button to open the Connection Settings dialog.

Connection Settings				
<ul> <li>Configure Proxies to Access the Internet</li> <li>No proxy</li> <li>Auto-detect proxy settings for this network</li> <li>Manual proxy configuration:</li> </ul>				
HTTP Proxy:	192.168.5.110	<u>P</u> ort:	8080 🗘	
	Use this proxy server for al	protocol	s	
<u>S</u> SL Proxy:	192.168.5.10	P <u>o</u> rt:	8080 😂	
ETP Proxy:	ETP Proxy: 192.168.5.110 Po <u>r</u> t: 8		8080 🗘	
<u>G</u> opher Proxy:	Gopher Proxy: 192.168.5.10 Port: 8080 🗘			
SO <u>C</u> KS Host:	SOCKS Host: 192.168.5.10 Port: 8080			
	○ SOCKS v4 ③ SOCKS v5			
<u>N</u> o Proxy for:	localhost, 127.0.0.1			
Example: .mozilla.org, .net.nz, 192.168.1.0/24 <u>A</u> utomatic proxy configuration URL:				
Reload				
	OK Can	cel	Help	

Screenshot 14 - Mozilla Firefox: Connection Settings dialog

- 4. Select Manual proxy configuration.
- 5. Uncheck Use this proxy server for all protocols checkbox.

6. Key in the proxy server IP address and the port used (Default 8080) in the HTTP Proxy, FTP Proxy and related Port text boxes.



If WPAD is enabled in GFI WebMonitor proxy settings, select **Auto-detect proxy** settings for this network. For more information, refer to the Enabling WPAD in Proxy Settings section in this manual.

- 7. Click OK to close Connection Settings dialog.
- 8. Click OK to close Options dialog.

## Google Chrome

#### 1. Launch Google Chrome.

Soogle Chrome ×	<del>4</del>	Googl	e 👝 🗆 🗶
← → C ☆ http://tools.g	oogle.com/chrome/intl/en/welcome.html		▶ <b>□</b> - <b>⊁</b> -
🗋 Customize Links 📄 Free Hotmail [	🖞 Windows Marketplace 📄 Windows Media 📋	New tab New window	Ctrl+T Ctrl+N
Capelashrama		New incognito window	Ctrl+Shift+N
Goøgle chrome		<ul> <li>Always show bookmarks bar Full screen</li> </ul>	Ctrl+B F11
One box for everything	g Google Maps × New Tab.	History Bookmark manager Downloads	Ctrl+H Ctrl+Shift+B Ctrl+J
New Tab page		Clear browsing data Import bookmarks & settings	Ctrl+Shift+Del
Application shortcuts	Maps Search Google for Ions club Search Google for Ionsgate Street Vie	Options About Google Chrome Help	F1
View all features ∢		EXIC	

Screenshot 15 - Google Chrome: Customize and Control Google Chrome menu

#### 2. Click Customize and Control Google Chrome ► Options.

Google Chrome Options	x
Basics Minor Tweaks Under the Hood	
Allow all cookies	•
Show cookies	
Network	
Set up a proxy to connect to the network.	
Change proxy settings	
Web Content	
Notify me when a pop-up is blocked	
Google Gears: Change Google Gears settings	≡
Security	
You have chosen to open certain file types automatically after downloading. You can clear these settings so that downloaded files don't open automatically.	
Reset to default	s
Clos	se

Screenshot 16 - Google Chrome: Under the Hood tab

- 3. In the Google Chrome Options dialog, click Under the Hood tab.
- 4. Click Change proxy settings button to open Internet Properties dialog.

- 5. Select the **Connections** tab.
- 6. Click LAN settings button.

Local Area Network (LAN) Settings 🛛 🔹 💽					
-Automatic conf	iguration				
Automatic conf use of manual	iguration may ove settings, disable a	rride manu utomatic c	ual setting: onfiguratio	s. To ensure the on.	
Automatica	lly detect settings				
Use automa	atic configuration s	cript			
Address				]	
Proxy server -					
Use a proxy dial-up or V	y server for your L PN connections).	AN (These	settings (	will not apply to	
Address:	myproxy	Port:	8080	Advanced	
Bypass	proxy server for lo	cal addre:	sses		
			ОК	Cancel	

Screenshot 17 - LAN Settings dialog

7. Check Use a proxy server for your LAN checkbox.

8. Key in the proxy server name or IP address and the port used (Default 8080) in the Address and Port text boxes.



If WPAD is enabled in GFI WebMonitor proxy settings check the **Automatically detect settings** checkbox in the **Automatic configuration** area. For more information, refer to the Enabling WPAD in Proxy Settings section in this manual.

- 9. Click OK to close LAN Settings dialog.
- 10. Click OK to close Internet Options dialog.

# 4 Installing in Simple Proxy Mode

#### 4.1 Introduction

This chapter provides you with information related to the installation of GFI WebMonitor on a machine configured as a Proxy server.

#### 4.2 System Requirements

#### 4.2.1 Software

GFI WebMonitor in Simple Proxy mode can be installed on:

ТҮРЕ	SOFTWARE REQUIREMENTS
Supported Operating Systems	» Microsoft Windows Server 2003 (x86)
	» Microsoft Windows Server 2008 (x86 or x64)
	» Microsoft Windows Server 2008 R2 (x64)
	» Microsoft Windows XP SP2
	» Microsoft Windows Vista
	» Microsoft Windows 7
Other required components	» Microsoft Internet Explorer 7 or later
	» Microsoft.NET Framework 2.0
	» Microsoft Message Queuing Service (MSMQ)
	<ul> <li>Microsoft SQL Server 2000 or later (for reporting purposes)</li> </ul>

#### 4.2.2 Hardware

Minimum hardware requirements depend on the GFI WebMonitor edition.

EDITION	HARDWARE REQUIREMENTS
All Editions	<ul> <li>Router/gateway that supports traffic forwarding or port blocking</li> </ul>
WebFilter Edition	<ul> <li>» Processor: 2.0 GHz</li> <li>» RAM: 1 GB (Recommended 4GB)</li> <li>» Hard disk: 2 GB of available disk space</li> </ul>
WebSecurity Edition	<ul> <li>» Processor: 2.0 GHz</li> <li>» RAM: 1 GB (Recommended 4GB)</li> <li>» Hard disk: 10 GB of available disk space</li> </ul>
Unified Protection Edition	<ul> <li>» Processor: 2.0 GHz</li> <li>» RAM: 2 GB (Recommended 4GB)</li> <li>» Hard disk: 12 GB of available disk space</li> </ul>



Allocation of hard disk space depends on your environment. The size specified in the requirements is the minimum required to install and use GFI WebMonitor. The recommended size is between 150 and 250GB.

#### 4.3 Installation

#### 4.3.1 Pre-requisites

Before installing GFI WebMonitor on a Proxy server, the router/gateway must be configured to:

- » Block all outgoing HTTP/HTTPS traffic generated from the client machines
- » Allow outgoing HTTP/HTTPS traffic generated by GFI WebMonitor only
- » Allow Non-HTTP/HTTPS traffic generated from client machines.

In this environment, traffic forwarding can be used to forward HTTP/HTTPS traffic from the client machines to GFI WebMonitor machine. For more information, refer to the Configuring Commonly Used Routers section in this manual.

4. Ensure that the listening port (default 8080) is not blocked by your firewall. For more information on how to enable firewall ports on Microsoft Windows Firewall, refer to http://kbase.gfi.com/showarticle.asp?id=KBID003879

#### 4.3.2 Upgrades

In order to upgrade GFI WebMonitor, obtain the latest version from http://www.gfi.com/pages/webmon-selection-download.asp.



The upgrade process is similar to the installation instructions. For more information, refer to the Installation Procedure section in this chapter.

If installing a new version of GFI WebMonitor on a different infrastructure, it is recommended to uninstall GFI WebMonitor before installing the new version.

#### 4.3.3 Installation Procedure

Run the installer as a user with administrative privileges on the target machine.

1. Double click the GFI WebMonitor executable file.

2. If the current version of Microsoft .NET Framework is not compatible with the required version, a warning dialog will be displayed. Click **OK**. This will stop the installation process. Install the required Microsoft .NET Framework version and start the installation of GFI WebMonitor again.

3. Choose whether you want the installation wizard to search for a newer build of GFI WebMonitor on the GFI website and click **Next**.

4. Read the licensing agreement. To proceed with the installation select I accept the terms in the license agreement and click Next.

🔂 GFI WebMonitor 2011 - InstallShield Wizard
WebMonitor Configuration - Access Permissions         Specify who will be able to access the GFI WebMonitor Web interface.
By default only an administrator logged in on this computer will be authorized to access the GFI WebMonitor web interface. GFI WebMonitor can be configured to allow other users/computers to access its web based interface over the network.
Enter the user name or the computer IP which will be granted access to GFI WebMonitor:
127.0.0.1;192.168.3.81;192.168.200.7;192.168.3.81
NOTE: Specify username(s) in the format DOMAIN\username.
NOTE: The IP of this computer is already added to the access permission list.
NOTE: You can specify more than one user/computer. Separate entries with a semicolon (;) eg. 127.0.0.1;COMPANY\user1;COMPANY\user2;172.16.135.16
Install5hield
< Back Next > Cancel

Screenshot 18 - Installation: Access Permissions

5. Key in the user name or the IP address that will be used to access the web interface of GFI WebMonitor and click **Next**.



More than one user or machine can be specified. Separate entries with semicolons ';'

🕏 GFI WebMonitor 2011 - InstallShield Wizar	i 🛛 🔀
<b>Customer Information</b> Please enter your information.	GF
<u>U</u> ser Name: Bob Jones <u>O</u> rganization: myCompany	
License Key: Evaluation InstallShield < Back	Next > Cancel

Screenshot 19 - Installation: Customer Information

6. Key in the **User Name** and **Organization**. If you have a license key, update the **License Key** details and click **Next**.



The license key can be keyed in after installation or expiration of the evaluation period of GFI WebMonitor. For more information, refer to the Entering Your License Key After Installation section in this manual.

🙀 GFI WebMon	itor 2011 - InstallShield Wizard 🛛 🛛 🛛						
Service Logon	Information						
The following logon information is used by the WebMonitor Service							
The GFI WebM functionality. F privileges. Plea expire. For dor	Ionitor service needs to run with administrative privileges for proper Ilease enter the username and password of an account with administrative use make sure that the account is active and does not have the password set to mains, user names must be in the format of DOMAIN\UserName.						
User Name:	administrator						
Password:	*****						
NOTE: The username and password provided must have "Logon As Service" rights. If it doesn't it will be switched ON automatically for the specified account. These credentials will only be used to create and run as new service in the services control panel. InstallShield							
	< Back Next > Cancel						

Screenshot 20 - Installation: Service Logon Information

7. Key in the logon credentials of an account with administrative privileges and click Next.

The user account must have **Log on as a service** rights. For more information, refer to the Assigning Log On As A Service Rights section in this manual.

😼 GFI WebMonito	r 2011 - InstallShield Wizard	×
Mail Settings Enter administrato	r email and SMTP mail server settings	
Please enter the d WebMonitor 2011	etails of the SMTP server and email address that are to be used by GFI for email reporting.	
From:	WebMonitor@127.0.0.1	
To:	Administrator@127.0.0.1	
SMTP Server:	127.0.0.1 Port: 25	
InstallShield	Verify Mail Settings < <u>B</u> ack <u>N</u> ext > Cancel	

Screenshot 21 - Installation: Mail Settings

8. Provide the SMTP mail server details and email address to which administrator notifications will be sent. Select **Verify Mail Settings** to send a test email. Click **Next**.

9. Click Next to install in default location or click Change to change installation path.

10. If the Microsoft Message Queuing Service (MSMQ) is not installed, a message will prompt the user that the installation requirements have not been met. Click **Next** to install the service automatically.

11. Click Install to start the installation and wait for the installation to complete.

12. Click Finish.

13. After the installation, **GFI WebMonitor Configuration Wizard** is launched automatically. This will help you configure the server in simple proxy mode.

14. In the welcome screen, click Next.

15. Select Simple proxy mode as your network environment and click Next.



To view help on how to configure most commonly used routers, select the **Click here** link. For more information, refer to the **Configuring Commonly Used Routers** section in this manual.

16. Click **Finish** to apply proxy settings.

#### 4.3.4 Post-installation Test

To test the installation from the machine where GFI WebMonitor was installed:

- » Option 1: Click Start ► Programs ► GFI WebMonitor ► GFI WebMonitor. Further information can be found in the section entitled Launching GFI WebMonitor in this document.
- » **Option 2:** Key in the URL http://monitor.isa in a web browser on the same machine.



If using the GFI WebMonitor through the web browser interface on the same machine, Internet Explorer must be configured to use a proxy server. For more information refer to Microsoft Internet Explorer section in this manual.

To test GFI WebMonitor installation from machines of users and/or IP addresses that were allowed access to the application during installation:

» Key in the URL http://monitor.isa in a web browser from their machine. The Internet browser must be configured to use specific proxy settings to enable this access.

#### 4.4 Post-installation Actions: Configure Proxy Settings

Configure the user machines to use GFI WebMonitor machine as the default proxy. This can be achieved by:

- » **Option 1:** Configuring the client machines using the Group Policy object (GPO) feature within the Active Directory.
- » Option 2: Configuring Internet browsers to use specific proxy settings on each client machine manually.



If WPAD is enabled, the client internet browser can be configured to detect the proxy settings automatically. For more information, refer to the Enabling WPAD in Proxy Settings section in this manual.

#### 4.4.1 Configuring GFI WebMonitor Machine as the Default Proxy Using GPO in Microsoft Windows Server 2003

To configure the **Proxy Settings** on all client machines to use GFI WebMonitor as a proxy server through Microsoft Windows Server 2003 GPO:

1. Navigate to **Start** ► **Programs** ► **Administrative Tools** ► **Active Directory Users and Computers** on the Domain Controller.

2. Under the domain node, right-click the organizational unit where you wish to apply the group policy and click **Properties**.



to apply the group policy to all the computers on the domain, right-click on the domain node directly and click **Properties**.

masterdomain.com Properties	? ×						
General Managed By Group Policy							
To improve Group Policy management, upgrade to the Group Policy Management Console (GPMC).							
Current Group Policy Object Links for masterdomain							
Group Policy Object Links No Override Disabled							
Group Policy Objects higher in the list have the highest priority. This list obtained from: win2k3serv.masterdomain.com							
New Add Edit Up	]						
Options         Delete         Properties         Down							
□ <u>B</u> lock Policy inheritance							
OK Cancel Apply							

Screenshot 22 - 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.

🚡 Group Policy Object Editor		
Eile       Action       Yiew       Help         ←       →       €       III       E       III         S       Default Domain Policy [win2k3serv.masterdomain.com] Polic       IIII       IIIII       IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Name Browser User Interface	Description Title, bitmaps, logos, etc. Connection settings, proxy and
Windows Settings     Administrative Templates     User Configuration     Software Settings     Windows Settings     Windows Settings     Scripts (Logon/Logoff)     Security Settings     Folder Redirection     Folder Redirection     Administrative Templates	DRLs Security	Favorites, Links and Important Zones & Ratings and Authenticode Default program settings and ex

Screenshot 23 - GPO Editor window

5. Expand User Configuration ► Windows Settings ► Internet Explorer Maintenance ► Connection and double-click Proxy Settings to open the Proxy Settings dialog.

Prox	y Settings						? ×
Pro	xy Settings						
Ye se	ou can specify eparate entrie	y what proxy servers, if any, you es.	u want y	your user	's to (	o connect to. Use semicolons ( ; ) to	
F	Enable pro:	xy settings					
Г	Proxy Server	′s				Exceptions	- II
		Address of proxy		Port		Do not use proxy server for	
	<u>1</u> . HTTP:	192.168.5.110	:	8080		addresses beginning with:	
	2. Secure:	192.168.5.10	:	8080			
	<u>3</u> , FTP:	192.168.5.110	:	8080			
	<u>4</u> . Gopher:	192.168.5.10	:	8080			
	<u>5</u> . Socks:	192.168.5.10	:	8080			
	Use the	same proxy server for all addres	ses			I Do not use proxy server for local (intranet) addresses.	
				ЭК		Cancel Apply Help	

Screenshot 24 - Proxy Settings dialog

6. Check Enable proxy settings checkbox.

7. Uncheck Use the same proxy server for all addresses checkbox.

8. Key in the proxy server IP address and the port used (Default 8080) in the HTTP and FTP text boxes.

9. Click **OK** to apply changes.

10. Close all open windows.

#### 4.4.2 Configuring GFI WebMonitor Machine as the Default Proxy Using GPO in Microsoft Windows Server 2008

To configure the **Proxy Settings** on all client machines to use GFI WebMonitor as a proxy server 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.

ap-in	Vendor 🔺		Console Root		Edit Extensions
Device Manager	Microsoft		Group Policy Ma	nagement	
Disk Management	Microsoft				Remove
DNS	Microsoft			1	
Event Viewer	Microsoft				Move Up
Exchange Server 2007	Microsoft			-	
Folder	Microsoft 🦳				Move Down
Group Policy Management	Microsoft	Add >		1	
Group Policy Management E	Microsoft				
Group Policy Object Editor	Microsoft				
Group Policy Starter GPO Ed	Microsoft				
Internet Information Servic	Microsoft (				
Internet Information Servic	_				
IP Security Monitor	Microsoft (				Advanced
			I		Auvanceum
ription:					

Screenshot 25 - Add/Remove Snap-ins window

#### 3. Select Group Policy Management from the Available snap-ins list, and click Add.

4. Click OK.

🚟 Console1 - [Console Root\Group Policy	Management\Forest: techcom.com\Domains\techcom.com ]
🚟 File Action View Favorites Window	Help
🗢 🔿 🗡 💼 🗎 🖬 🧟 🔽 🖬	
Console Root Group Policy Management A Excest: techcom com	techcom.com Linked Group Policy Objects Group Policy Inheritance Delegation
	Link Order A GPO Enforced Link Enabled GPO
i Derault Domain Policy	
Group Policy Objects     WMI Filters      Starter GPOs	▼

Screenshot 26 - Console Root domain window

5. Expand **Group Policy Management** ► **Forest** ► **Domains** and **<domain>**, then select the organizational unit where you wish to apply the group policy.



To apply the group policy to all the computers on the domain, select the domain node directly.

6. Right-click **Default Domain Policy** and click **Edit** to open the **Group Policy Management Editor**.



Screenshot 27 - GPO Editor window

7. Expand User Configuration ► Policies ► Windows Settings ► Internet Explorer Maintenance ► Connection and double-click Proxy Settings to open the Proxy Settings dialog.

Proxy Set	ttings								? ×
Proxy Se	ttings								
You car separat	n specify te entrie able prox	y what proxy servers, if any, you es. Gopher cannot be customized xy settings	u want y I in Inter	our users net Explo	s to c orer 7	:onnect 7.	to. Us	e semicolons (	(; ) to
Proxy	y Server	'S			_	Exce	ptions		
		Address of proxy		Port		Don	iot use	proxy server	for
1. H	ITTP:	192.168.5.110	:	8080		addr	esses	beginning with	1:
2. S	ecure:	192.168.5.10	:	8080					<u>^</u>
3. F	TP:	192.168.5.110	:	8080					
4. G	opher:	192.168.5.10	:	8080					
5. S	ocks:	192.168.5.10	:	8080					×
	Use the	same proxy server for all addres	sses				Do not local (i	t use proxy ser ntranet) addre	esses.
			0	Ж		Cancel		Apply	Help

Screenshot 28 - Proxy Settings dialog

8. Check Enable proxy settings checkbox.

9. Uncheck Use the same proxy server for all addresses checkbox.

10. Key in the proxy server IP address and the port used (Default 8080) in the HTTP and FTP text boxes.

- 11. Click **OK** to apply changes
- 12. Close Proxy Settings dialog.
- 13. Close Group Policy Management Editor dialog and save the management console created.



When using Active Directory, the administrator can disable the Internet connection settings tab from the client machines. For more information, refer to the Disabling Internet Connections Settings on Client Machines section in this manual.

#### 4.4.3 Configuring Internet Browsers to Use a Proxy Server

You can also configure each individual user machine manually to set the GFI WebMonitor machine as the default proxy. This section shows how to configure the most commonly used Internet browsers to use a proxy server.

#### Microsoft Internet Explorer

- 1. Launch Microsoft Internet Explorer.
- 2. From the Tools menu, choose Internet Options and select the Connections tab.
- 3. Click LAN settings button.

Local Area Net	work (LAN) Se	ttings		? 🔀
Automatic conf Automatic conf use of manual	iguration iguration may over settings, disable au lly detect settings	rride manu utomatic c	ual settings. onfiguration.	To ensure the
Use automa Address	atic configuration s	cript		
Proxy server Use a proxy dial-up or V	y server for your L. PN connections).	AN (These	settings will	not apply to
Address:	myproxy proxy server for lo	Port: ocal addre:	8080 ( sses	Advanced
			ок	Cancel

Screenshot 29 - LAN Settings dialog

4. Check Use a proxy server for your LAN checkbox.

5. Key in the proxy server name or IP address of the GFI WebMonitor machine and the port used (Default 8080) in the **Address** and **Port** text boxes.



- 6. Click OK to close LAN Settings dialog.
- 7. Click OK to close Internet Options dialog.

#### Mozilla Firefox

- 1. Launch Mozilla Firefox.
- 2. Click **Tools** ► **Options** ► **Advanced** tab ► **Network** tab.
| Options   |  |         |  |         |          |              | × |
|---|--|---------|--|---------|----------|--------------|---|
| Main  | Tabs   | Content |  | Privacy | Security | Advanced     |   |
| General Network Update Encryption   |  |         |  |         |          |              |   |
| Conne   | Connection<br>Configure how Firefox connects to the Internet |         |  |         |          |              |   |
| Offline<br>Use u  | Offline Storage Use up to 50 SMB of space for the cache      |         |  |         |          |              |   |
| ✓ Iell me when a website asks to store data for offline use       Exceptions         The following websites have stored data for offline use: |  |         |  |         |          |              |   |
|   |  |         |  |         |          |              |   |
| Remove  |  |         |  |         |          |              |   |
|   |  |         |  | ок      | Cancel   | <u>H</u> elp |   |

Screenshot 30 - Mozilla Firefox: Options dialog

3. Click Settings button to open the Connection Settings dialog.

Connection Settings					
Configure Proxies to Access the Internet No proxy Auto-detect proxy settings for this network Manual proxy configuration:					
HTTP Proxy:	192.168.5.110	<u>P</u> ort:	8080 🗘		
	Use this proxy server for all protocols		s		
<u>S</u> SL Proxy:	192.168.5.10	P <u>o</u> rt:	8080 😂		
ETP Proxy:	192.168.5.110	Po <u>r</u> t:	8080 🗘		
<u>G</u> opher Proxy:	192.168.5.10	Port:	8080 🗘		
SO <u>C</u> KS Host:	192.168.5.10	Por <u>t</u> :	8080 🗘		
	○ SOCKS v4   SOCKS v5				
<u>N</u> o Proxy for:	localhost, 127.0.0.1				
Example: .mozilla.org, .net.nz, 192.168.1.0/24  Automatic proxy configuration URL:					
	OK Can	icel	Help		

- 4. Select Manual proxy configuration.
- 5. Uncheck Use this proxy server for all protocols checkbox.

6. Key in the proxy server IP address and the port used (Default 8080) in the HTTP Proxy, FTP Proxy and related Port text boxes.



If WPAD is enabled in GFI WebMonitor proxy settings, select **Auto-detect proxy** settings for this network. For more information, refer to the Enabling WPAD in Proxy Settings section in this manual.

- 7. Click OK to close Connection Settings dialog.
- 8. Click OK to close Options dialog.

# Google Chrome

1. Launch Google Chrome.



Screenshot 32 - Google Chrome: Customize and Control Google Chrome menu

2. Click Customize and Control Google Chrome > Options.

Google Chrome Options	x
Basics Minor Tweaks Under the Hood	
Allow all cookies	•
Show cookies	
Network	
Set up a proxy to connect to the network.	
Change proxy settings	
Web Content	
Notify me when a pop-up is blocked	
Google Gears: Change Google Gears settings	≡
Security	
You have chosen to open certain file types automatically after downloading. You can clear these settings so that downloaded files don't open automatically.	
Reset to default	5
	se

Screenshot 33 - Google Chrome: Under the Hood tab

- 3. In the Google Chrome Options dialog, click Under the Hood tab.
- 4. Click Change proxy settings button to open Internet Properties dialog.
- 5. Select the **Connections** tab.
- 6. Click LAN settings button.

Local Area Network (LAN) Settings 🛛 ? 🔀				
Automatic configuration Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.				
Automatically detect settings				
Use automatic configuration script				
Address				
Proxy server				
Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).				
Address: myproxy Port: 8080 Advanced				
Bypass proxy server for local addresses				
OK Cancel				

7. Check Use a proxy server for your LAN checkbox.

8. Key in the proxy server name or IP address and the port used (Default 8080) in the Address and Port text boxes.



If WPAD is enabled in GFI WebMonitor proxy settings check the **Automatically detect settings** checkbox in the **Automatic configuration** area. For more information, refer to the **Enabling WPAD** in **Proxy Settings** section in this manual.

- 9. Click OK to close LAN Settings dialog.
- 10. Click OK to close Internet Options dialog.

# 5 Launching GFI WebMonitor

# 5.1 Introduction

This chapter provides you with information related to the launching of GFI WebMonitor and an overview of the application's console.

### 5.2 Launching GFI WebMonitor

To launch GFI WebMonitor, navigate to **Start** ► **Programs** ► **GFI WebMonitor** ► **GFI WebMonitor**.

#### 5.3 Navigating the Console

GFI WebMonitor's console provides you with all the administrative functionality to monitor and manage network internet traffic.

GFI WebMonitor						_ 8 ×
GFI WebMonitor						
	2 Hide Controls <<					
GFI WebManitor	Last Blocked Requests	Top Categories By Bandwidth Top Categories By Sites F Hits and Bandwidth Chart	Tap Toda	Blocked Categories ay's Statistics	Hits Over Time Bendwidth Usage Trends	
Whitelist	WebSecurity: Cvaluation WebFilter:	Evaluation (10 days left)			Rutorefresh every	30 💌 seconds 🕏
Biocking WebFilter Edition	Today's Statistics		~ ×	Hits and Bandwidth Ch	art	^ X
WebSecurity Edition	Today's Statistics			100		300
D D Configuration	Processed Requests:	248		80 -	Δ.Δ.	- 250
A Licensing	Total Bandwidth Consumed:	272.78 MB		40	N \	- 200 👮
To Version Information	Current Active Connections:	2		2		- 150 💆
b 🙀 Quarantine	AV Scanned Downloads:	×		= 40 -		- 100 Å
() Hale		Quarantined Blocked		20 -		
(C) Help	AV & Anti-Phishing:	0 0			/ ·	~ -
	Download & Mt	0 0		8 8 8 8 8 8	200 190 190 190 190 190 190 190 190 190 1	
	Web Filtering:	0 0		88888	888888888888888888888888888888888888888	888
	L			1		

Screenshot 35 - GFI WebMonitor console view

**1** Navigation Bar - The navigation bar is located on the left-hand side of the console, and contains a number of nodes used to view and configure settings. The available nodes are:

- » Dashboard A graphical overview of GFI WebMonitor activity.
- » Monitoring Enables generation of several reports.
- » Whitelist/Blacklist Permanent and/or temporary whitelisting and blacklisting functions.
- » WebFilter Edition Provides access management for specific website categories for users, groups and IP addresses during specified periods.
- WebSecurity Edition Provides access management and control restrictions to web applications for users, groups and IP addresses.
- Configuration Provides configuration settings and administrative features for GFI WebMonitor.
- » Licensing and Version Information Provides access to the licensing setup and version information.
- » **Quarantine** Provides configuration and management of quarantined items that were blocked by GFI WebMonitor.

» Help - Provides help on all aspects of GFI WebMonitor's functionality.

**2** Viewing Pane - The viewing pane is located on the right-hand side of the console, and enables the administrator to view and configure settings according to the node selected from the Navigation Bar.

# 6 Miscellaneous

# 6.1 Introduction

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

# 6.2 Entering Your License Key After Installation

After installing GFI WebMonitor, you can enter your license key without re-installing or reconfiguring the application.

To enter your license key:

- 1. Navigate to the Licensing node.
- 2. In the License Key text box, key in the license key provided by GFI Software Ltd..
- 3. Click Save Settings.

#### 6.3 Enabling WPAD in Proxy Settings

To allow client browsers to detect proxy settings automatically, Web Proxy AutoDiscovery (WPAD) can be enabled within GFI WebMonitor.

To enable WPAD:

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

Configure the net	vork interface and port on which the proxy listens to incoming connections.	
192.168.200.7	8080	
Listen on all r	etwork interfaces	
Use WPAD fo	r network clients	
💿 Publish th	e IP of the GFI WebMonitor proxy in WPAD	
🔘 Publish th	e host name of the GFI WebMonitor proxy in WPAD	
NOTE: Provy will:	always listen for web connections from this computer (127.0.0.1:8080)	

Screenshot 36 - Configuration: Proxy Settings ► General view - Network Configuration

# 2. From the **Network Configuration** area, select the **Use WPAD for network clients** to allow client machines to detect the server as the default proxy.

3. Select:

OPTION	DESCRIPTION
Publish the IP of the GFI WebMonitor proxy in WPAD	Includes the GFI WebMonitor IP address in the WPAD.dat file
Publish the host name of the GFI WebMonitor proxy in WPAD	Includes the GFI WebMonitor host name in the WPAD.dat file

4. Click **Save Settings** to finalize enabling WPAD.

# 6.4 Refreshing Cached Microsoft Internet Explorer Settings

Microsoft Internet Explorer may cache previously configured Internet settings. To ensure that the updated Internet settings are automatically detected by a client browser:

- 1. Launch Microsoft Internet Explorer on the client machine.
- 2. From the Tools menu, choose Internet Options and select the Connections tab.
- 3. Click LAN settings button.
- 4. Uncheck Automatically detect settings checkbox.
- 5. Click OK to close LAN Settings dialog.
- 6. Click OK to close Internet Options dialog.
- 7. Restart Internet Explorer.
- 8. Repeat steps 2 to 3.
- 9. Check Automatically detect settings checkbox.
- 10. Click OK to close LAN Settings dialog.
- 11. Click OK to close Internet Options dialog.
- 12. Restart Internet Explorer to refresh the cached Internet Explorer settings.

For more information visit:

http://technet.microsoft.com/en-us/library/cc302643.aspx

# 6.5 Configuring Chained Proxy

Client machines can be configured to forward web traffic to the GFI WebMonitor server. In addition, the GFI WebMonitor server forwards the filtered traffic to a proxy server.

To configure GFI WebMonitor to forward web traffic to another proxy machine:

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

VebMonitor Proxy	will route the web traffic to	the following proxy:	
Address:	Port:		
Use the follo	wing user credentials as an	alternative to the default p	proxy authentication credentials.
(Leave blank	to disable atternative auther	tication)	
Username:	P	assword:	
Test Proxy Cl	aining		

Screenshot 37 - Configuration: Chained Proxy

2. From the **Chained Proxy** area, 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.



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.

#### 6.6 Configuring Routing and Remote Access

When installing GFI WebMonitor in Gateway mode on a Microsoft Windows Server 2003 or Microsoft Windows Server 2008, the Routing and Remote Access must be configured to use Network Address Translation (NAT). This can be done by:

1. Navigate to Start > Programs > Administrative Tools > Routing and Remote Access.

2. Right-click the <machine name> and select Configure and Enable Routing and Remote Access.

- 3. Click Next in the Routing and Remote Access Server Setup Wizard dialog.
- 4. Select Network address translation (NAT) and click Next.

Routing and Remote Access Serv	touting and Remote Access Server Setup Wizard				
NAT Internet Connection       You can select an existing interface or create a new demand-dial interface for client computers to connect to the Internet.         Image: Use this public interface to connect to the Internet:					
Name	Description	IP Address			
External (WAN) Internal (LAN)	Microsoft Virtual Machi Microsoft Virtual Machi	(DHCP) 192.168.5.100			
<ul> <li>Create a new demand-dial A demand-dial interface is a option if this server connect over Ethernet. The Deman</li> <li>Enable security on the sele Basic Firewall prevents una through the Internet.</li> </ul>	<ul> <li>Create a new demand-dial interface to the Internet         <ul> <li>A demand-dial interface is activated when a client uses the Internet. Select this option if this server connects with a modem or by using the Point-to-Point Protocol over Ethernet. The Demand-Dial Interface Wizard will start at the end of this wizard.</li> <li>Enable security on the selected interface by setting up Basic Firewall.             Basic Firewall prevents unauthorized users from gaining access to this server through the Internet.</li> </ul> </li> <li>For more information about network interfaces, see <u>Routing and Remote Access Help</u>.</li> </ul>				
	< <u>B</u> ack	Next > Cancel			

Screenshot 38 - Microsoft Windows Server 2003: Routing and Remote Access Server Setup Wizard dialog

5. Select Use this public interface to connect to the Internet.

- 6. Select the network card connected to the external network and click Next.
- 7. Click Finish.

To confirm that the Routing and Remote Access service is started:

- 1. From command prompt, key in services.msc
- 2. Check that the status of the Routing and Remote Access service is Started.

# 6.7 Configuring Commonly Used Routers

When installing GFI WebMonitor in Simple Proxy mode, the router must support port blocking or traffic forwarding. This sub-section contains information on how to configure some of the most commonly used routers.

# 6.7.1 SonicWall TZ 180

On **SonicWall TZ 180**, ports are blocked by creating firewall access rules.

# Step 1: Creating a New Firewall Service for Port 80

To create a new firewall service for port 80:

- 1. Open the web configuration page from an internet browser.
- 2. Provide any credentials required.

C SonicWALL - Administr	ation for 001/CS2ASS98			
SONICWALL	COMPRESSIVE INTERNET SECURITY-			
System Network Firewall	Firewall > Services			
Access Dulas	Custom Services			
Advanced	Name P	ort Start Port End	Protocol	Enabl
Services	No Entries			
VolP	Add			
Connections Monitor	Default			
	Name	Port Start	Port End	Protoco
	Authentical Name: HTTP	113	113	TCP
	Chat (IRC) Port Range: 80 - 80	194	194	TCP
	Chat (IRC) Protocol: TCP(6) -	6666	6666	TCP
	Chat (IRC)	6667	6667	TCP
	Chat (IRC) OK Ca	ncel 6668	6668	TCP
	Chat (IRC)	6669	6669	TCP
	Chat (RC)	6670	6670	TCP
	Chat (IRC) antenet protected model off	7000	7000	TCP
	Citrix	1494	1494	TCP
	Citrix	1604	1604	UDP
	Echo	7	7	TCP
	Echo	7	7	UDP
	Enhanced TV	9000	9000	TCP
	File Transfer (FTP)	21	21	TCP
VPN	Filemaker	5003	5003	TCP
Users	Filemaker	5003	5003	UDP
curity Services	Gatekeeper (H323)	1718	1718	UDP
Log	Gatekeeper (H323)	1719	1719	UDP
Mirarde	Gopher	70	70	TCP

Screenshot 39 - SonicWall: Services view and Add Service dialog

- 3. From the router's configuration web interface, click **Firewall > Services**
- 4. Click Add to open the Add Service console.
- 5. Key in a name in the Name text box, for example "HTTP".
- 6. In Port Range, key in 80-80.

- 7. From the Protocol drop-down list, select TCP.
- 8. Click OK.

# Step 2: Blocking the New Service

To create a firewall access rule to block the newly created service:

- 1. Open the web configuration page from an internet browser.
- 2. Provide any credentials required.
- 3. From the router's configuration web interface, click **Firewall** ► **Access Rules**.
- 4. Click Add button to open the Add Rule console.

실 http://192.168.168	3.168/ - Edit Rule -	Windows Internet Explorer	
General	Advanced	Bandwidth	
Rule Settin	gs		
Action:	🔘 Allow 🧕	Deny	
Service:	Web (HTTF	²) <b>▼</b>	
	Ethernet:	Address Range Begin:	Address Range End:
Source:	LAN 👻	*	
Destination:	WAN -	*	
Comment			
Comment			
Comment			
Ready			
		0	K Cancel Help

Screenshot 40 - SonicWall: Edit Rule dialog

- 5. Select the General tab.
- 6. From the Action radio buttons, select Deny.
- 7. From the Service drop-down list, select Web (HTTP).

8. In the **Source** row, select **LAN** from the **Ethernet** drop-down list, and key in "\*" in **Address Range Begin** text box.



By selecting the wildcard "\*", all inbound network traffic and all IP ranges on port 80 are blocked.

9. In the **Destination** row, select **WAN** from the **Ethernet** drop-down list and key in "\*" in **Address Range Begin** text box.

10. (Optional) Select the Advanced tab to configure a time-based schedule.

# Step 3: Creating a Firewall Access Rule to Allow HTTP Traffic From GFI WebMonitor Proxy

To create a firewall access rule to allow Web (HTTP) traffic originating from GFI WebMonitor Proxy machine:

- 1. Open the web configuration page from an internet browser.
- 2. Provide any credentials required.
- 3. From the router's configuration web interface, click **Firewall** ► **Access Rules**.
- 4. Click Add button to open the Add Rule console.

실 http://192.168.168.	168/ - Edit Rule - 1	Windows Internet Explorer	
General	Advanced	Bandwidth	
Rule Setting	js		
Action:	Allow C	Deny	
Service:	Web (HTTP	) 🗸	
	Ethernet:	Address Range Begin:	Address Range End:
Source:	LAN 👻	192.168.2.200	
Destination:	WAN 👻	*.	
Comment			
Comment			
Ready			
		O	K Cancel Help

Screenshot 41 - SonicWall: Edit Rule dialog

- 5. Select the General tab.
- 6. From the Action radio buttons, select Allow.
- 7. From the Service drop-down list, select Web (HTTP).

8. In the **Source** row, select **LAN** from the **Ethernet** drop-down list, and key in the IP address of the GFI WebMonitor proxy machine in **Address Range Begin** text box.

9. In the **Destination** row, select **WAN** from the **Ethernet** drop-down list and key in "\*" in **Address Range Begin** text box.

- 10. (Optional) Select the Advanced tab to configure a time-based schedule.
- 11. Click **OK** button.

# Step 4: Traffic Forwarding to GFI WebMonitor Proxy

To forward network traffic through the GFI WebMonitor Proxy:

- 1. Open the web configuration page from an internet browser.
- 2. Provide any credentials required.



Screenshot 42 - SonicWall: Automatic Proxy Forwarding view

3. From the router's configuration web interface, click **Network** ► **Web Proxy**.

4. In the **Proxy Web Server (name or IP address)** text box, key in the IP address of the GFI WebMonitor proxy machine

- 5. In the Proxy Web Server Port text box, key in the port used (Default 8080).
- 6. Click Apply button.

# 6.7.2 SonicWall NSA 2400

On SonicWall NSA 2400 two steps are required to:

- » Define the external and internal network cards
- » Create traffic controlling firewall rules

# Step 1: Defining Network Addresses

To define the external and internal network cards:

- 1. Open the web configuration page from an internet browser.
- 2. Provide any credentials required.

#### Address Objects

Add	Delete Refresh P	urge		
<b>•</b> #	Name	Address Detail	Туре	Zone
1	X0 IP	192.168.168.168/255.255.255.255	Host	LAN
2	X0 Subnet	192.168.168.0/255.255.255.0	Network.	LAN
<b>m</b> 3	X1IP	192.168.100.148/255.255.255.255	Host	WAN
<b>II</b> 4	X1 Subnet	192.168.100.0/255.255.255.0	Network	WAN
s s	X2 IP	0.0.0/255.255.255.255	Host	
6	X2 Subnet	0.0.0.0/255.255.255.0	Network	
7	X3IP	0.0.0/255.255.255.255	Host	
<b>1</b> 8	X3 Subnet	0.0.0/255.255.255.0	Network	
9	X4 IP	0.0,0.0/255.255.255.255	Host	
10	X4 Subnet	0.0.0.0/255.255.255.0	Network	
11	X5 IP	0.0.0/255.255.255.255	Host	
12	X5 Subnet	0.0.0/255.255.255.0	Network	
13	Default Gateway	192, 168, 100, 1/255, 255, 255, 255	Host	WAN
14	Secondary Default Gateway	0.0.0.0/255.255.255.255	Host	WAN
15	WLAN RemoteAccess Networks	0.0.0.0/0.0.0.0	Network	VPN
16	WAN RemoteAccess Networks	0.0,0.0/0.0.0.0	Network	VPN
17	192.168.100.148	192.168.100.148/255.255.255.255	Network	WAN
18	proxy	192, 168, 168, 65/255, 255, 255, 255	Host	LAN

Screenshot 43 - SonicWall: Address Objects view

- 3. From the router's configuration web interface, click Network > Address Objects
- 4. Click Add button to add a WAN connection
- 5. In the Address Detail column, key in the IP address of the external network card.
- 6. In the Type column, select Network.
- 7. In the **Zone** column, select **WAN**.
- 8. Click Add button to add a LAN connection
- 9. In the Address Detail column, key in the IP address of the internal network card.
- 10. In the Type column, select Host.
- 11. In the Zone column, select LAN.

#### Step 2: Creating Firewall Rules

To create traffic controlling firewall rules:

- 1. Open the web configuration page from an internet browser.
- 2. Provide any credentials required.

	Access F	ules										
t	Restore Defaults											
Ruies ed tings s	Access Rules (Al	l <b>l &gt; All.)</b> Rules Citie	etrix ODr	op-down Boxe	6							
tions Monitor	Add	00	Zone	Priority	Source	Destination	Service	Action	Users	Comment	Bhable	Configure
205 Mapping ISL Control	C LAN											00
	E 1 LAN	>	LAN	1	Any	AT X0 Management IP	SAMP	Allow	AI	ø	0	
n Firevall	E 2 LAN	×	LAN	2	Алу	All XO Management DP	Fing	Allow	Al	ø	0	
	E 3 LAN	>	LAN	3	Алу	All XO Management (P	SSH Management	Авон	Al	Ø	0	
	E 4 LAN	>	LAN	4	Any	All XO Management IP	HTTPS Management	Allow	AJ	ø	0	
itty					100	ATVO Managament /P	HTTP: Naciacientest	Allers	4	ø	0	
ity ices	S LAN	>	LAN	5	елу	An worker agement up	the real againstic	- PARA PA	144	14		
:5	E S LAN	>	LAN	5	Алу	Any	Any	Alles	AI	ø	0	
5		> >	LAN LAN WAN	5 6 1	Any Drboy	Any Any	Any HTTP	Alica	Al	ø	0	100 100
ity ices	5 LAN 6 LAN 7 LAN 0 U LAN	N N N N	LAN LAN WAN WAN	5 6 1 2	any Any procy proxy	Алу Алу Алу Алу	Any HTTP DNS (Name Service)	Allow Allow Allow	Al Al Al	ø	র ব	4 0 ×
5	5 LAN 6 LAN 7 LAN 0 LAN 9 LAN	> > > > >	LAN LAN WAN WAN	5 6 2 3	Any Any proxy proxy Any	Алу Алу Алу Алу Алу Алу	Any HTTP DNS (Name Service) Any	Allow Allow Allow Deny	Al Al Al	ø	ব ব ব ত	100 100 100 100
5	5         LAN           6         LAN           7         LAN           8         LAN           9         LAN           10         LAN	x x x x	LAN LAN WAN WAN WAN	5 6 2 3	Any Any proxy proxy Any WAN RemoteAccess Networks	Алу Алу Алу Алу Алу Алу	Any HTTP DNS (Herre Service) Any Any	Allow Allow Allow Deny Allow	Al Al Al Al Al	8	지 전 전 전	a 2 0 a 2 8 a 2 8 a 2 8

Screenshot 44 - SonicWall: Access Rules view

- 3. From the router's configuration web interface, click **Firewall** ► Access Rules.
- 4. Click Add button to add a new rule.
- 5. Repeat step 4 to create three rules with the following information:

ZONE	PRIORITY	SOURCE	DESTINATION	SERVICE	ACTION
LAN>WAN	1	Proxy	Any	HTTP	Allow
LAN>WAN	2	Proxy	Any	DNS	Allow
LAN>WAN	3	Any	Any	Any	Deny

# 6.7.3 Cisco ADSL Router Cisco 878 (MPC8272)

The **Cisco** command console enables the administrator to manage the router. Port 80 is blocked by executing an **Access-list** command.

The format of an access-list console command is:

access-list [Number] [Action] [Source] [Destination] [Port]

To deny access to port 80, key in the following command in the Cisco command console:

Access-list 100 deny any any eq 80

#### 6.7.4 Netgear Wireless Router DG834GT

On **Netgear Wireless Router DG834GT**, ports are blocked by creating firewall access rules. This section describes how to:

- » Create a firewall access rule to allow Web (HTTP) traffic originating from GFI WebMonitor Proxy machine
- » Create a firewall access rule to block all outgoing HTTP traffic

# Step 1: Creating a Firewall Access Rule to Allow HTTP Traffic From GFI WebMonitor Proxy

To create a firewall access rule to allow Web (HTTP) traffic originating from GFI WebMonitor Proxy machine:

- 1. Open the web configuration page from an internet browser.
- 2. Provide any credentials required.

NOTICES !	N E	GEAR Super Wireless ADSL	Router DG834GT
<ul> <li>Setup Wizard</li> </ul>	Â	Outbound Services	
Setup Basic Settings		Service	HTTP(TCP:80)
<ul> <li>ADSL Settings</li> <li>Wireless Settings Security</li> </ul>		Action LAN Users	ALLOW always
<ul> <li>Logs</li> <li>Block Sites</li> <li>Firewall Rules</li> </ul>			start 192 . 168 . 0 . 3 finish:
<ul> <li>Services</li> <li>Schedule</li> <li>E mail</li> </ul>		WAN Users	Any -
Maintenance Router Status	ш	Log	finish:
<ul> <li>Attached Devices</li> <li>Backup Settings</li> <li>Set Password</li> </ul>		Apply	Cancel

Screenshot 45 - Netgear Wireless Router DG834GT: Outbound Services view

- 3. From the router's configuration web interface, click **Firewall Rules** ► **Outbound Services**.
- 4. From the Service drop-down list, select HTTP (TCP80).
- 5. From the Action drop-down list, select ALLOW always.
- 6. From the LAN Users drop-down list, select Single address.
- 7. In the Start text box, key in the IP address of the GFI WebMonitor proxy machine
- 8. From the WAN Users drop-down list, select Any.
- 9. Click Apply to save settings.

# Step 2: Creating a Firewall Access Rule to Block All Outgoing HTTP Traffic

To create a firewall access rule to block all Web (HTTP) traffic:

- 1. Open the web configuration page from an internet browser.
- 2. Provide any credentials required.

N Same	ETGEAR Super Wirele	ess ADSL Router DG834GT	108 Mbps 2.4 GHz 802.11
<ul> <li>Setup Wizard</li> </ul>	Outbound Services		
Setup	Alter and a second seco		
Basic Settings	Service	HTTP(TCP:80)	
ADSL Settings	Action	BLOCK always	
Wireless Settings			
Security	LAN Users		Any -
Logs		start:	
Block Sites		finish	
Firewall Rules			·(·()
Services	WAN Users		Any -
Schedule		start .	
• E-mail		finish	
Maintenance		iinisii. []•[	•.
Router Status	Log		Always -
Attached Devices			
Backup Settings		Apply Cancel	
C ( D			

Screenshot 46 - Netgear Wireless Router DG834GT: Outbound Services view

- 3. From the router's configuration web interface, click **Firewall Rules** > **Outbound Services**.
- 4. From the Service drop-down list, select HTTP (TCP80).
- 5. From the Action drop-down list, select BLOCK always.
- 6. From the LAN Users drop-down list, select Any.
- 7. From the WAN Users drop-down list, select Any.
- 8. Click Apply to save settings.

# 6.7.5 DrayTek VIGOR 2820N ADSL2

On **DrayTek VIGOR 2820 series**, port 80 is blocked on all machines except the proxy by creating two firewall filter rules. To do this create the following two rules:

- First rule blocks IP addresses smaller than the GFI WebMonitor proxy machine IP address (excluding the proxy machine's IP address)
- » Second rule blocks IP addresses greater than the GFI WebMonitor proxy machine IP address (excluding the proxy machine's IP address)

By default the router, contains a pre-defined rule for NetBios DNS lookups. To view or configure the firewall rules:

- 1. Open the web configuration page from an internet browser.
- 2. Provide any credentials required.

eral Setup						
Call Filter	۲	Enable		Start Filter Set	Set#1 -	•
	0	Disable				
Data Filter	۲	Enable		Start Filter Set	Set#1 -	•
	0	Disable				
Application Filter IM/P2P Filter URL Content Filter Web Content Filter			Action/ Pass · None · None ·	/Profile		slog
Advance Setting  Accept large i	ncoming	fragmen	Edit	or ICMP packets (	for some	games, ex. CS )

Screenshot 47 - DrayTek: General Setup view

- 4. From the Start Filter Set drop-down lists of both Call Filter and Data Filter, select Set#1.
- 5. Click **OK** to save the changes
- 6. Select **Firewall** ► **Filter Setup** menu. This page contains the collection of rules.

Firewall >> Filter Setup						
Filter Se	etup		Set to Factory Default			
Set	Comments	Set	Comments			
1.	Default Call Filter	<u>7.</u>				
<u>2.</u>	Default Data Filter	<u>8.</u>				
<u>3.</u>		<u>9.</u>				
<u>4.</u>		<u>10.</u>				
<u>5.</u>		<u>11.</u>				
<u>6.</u>		<u>12.</u>				

Screenshot 48 - DrayTek: Filter Setup view

7. Select rule number 1 from the Set list to open the Edit Filter Set page.

Set 1 Rule 1		
Check to enable the Filter Rule	·	
Comments:	Block Range 1	
Index(1-15) in <u>Schedule</u> Setup:	,,,,	
Direction:	LAN -> WAN 🔻	
Source IP:	192.168.1.2~192.168.1.10	Edit
Destination IP:	Any	Edit
Service Type:	TCP, Port from any to 80	Edit
Fragments:	Don't Care 🗸	
Application	Action/Profile	Syslog
Filter:	Block Immediately -	
Branch to Other Filter Set:	None 🔻	
IM/P2P Filter:	None +	
URL Content Filter	None -	
Web Content Filter	None -	
Advance Setting	Edit	

Screenshot 49 - DrayTek: Edit Filter Rule view (IP addresses smaller than the GFI WebMonitor proxy machine IP address)

8. Double click the first rule (Block NetBios) to open the filter page.

9. In the filter page, click "1" to open the Filter Rule configuration

10. Key in a name, example "Block Range 1" in the **Comments** text box.

11. From the Direction drop-down list, select LAN->WAN.

12. Click Edit button of the Source IP field. This opens the IP Address Edit page.

Address Type	Range Address 🔹
Start IP Address	192.168.1.2
End IP Address	192.168.1.10
Subnet Mask	0.0.0
Invert Selection	
P Group	None 👻
or IP Object	None 👻
or IP Object	None 👻
or IP Object	None 👻

Screenshot 50 - DrayTek: IP Address Edit view

13. From the Address Type drop-down list, select Range Address.

14. In the **Start IP Address** text box, key in the smallest IP address of the range of IP addresses smaller than the GFI WebMonitor proxy machine IP address.

15. In the **End IP Address** text box, key in the largest IP address of the range of IP addresses smaller than the GFI WebMonitor proxy machine IP address (excluding the proxy machine's IP address).

16. Click **OK** to apply settings.

17. In the Edit Filter Rule page, click Edit button of the Service Type field.

Service Type	User	defined		×
Protocol	TCP	-	6	
Source Port	= •	1	~	65535
Destination Port	= +	80	~	80
Service Group	None	-		
or <u>Service Object</u>	1-prox	yService	• •	
or Service Object	None		*	
or Service Object	None		Ŧ	

Screenshot 51 - DrayTek: Service Type Edit view

- 18. From the Service Type drop-down list, select User defined.
- 19. From the **Protocol** drop-down list, select **TCP**.
- 20. In the **Source Port** text boxes, key in "1" and "65535" respectively.
- 21. In the **Destination Port** text boxes, key in "80" and "80" respectively.
- 22. Click **OK** to apply settings.

23. Repeat steps 1 to 22 to block IP addresses greater than the GFI WebMonitor proxy machine IP address (excluding the proxy machine's IP address).

r Set 1 Rule 2		
Check to enable the Filter Rule	No	
Comments:	Block Range 2	
Index(1-15) in <u>Schedule</u> Setup:		
Direction:	LAN -> WAN 👻	
Source IP:	192.168.1.12~192.168.1.255	Edit
Destination IP:	Any	Edit
Service Type:	TCP, Port from any to 80	Edit
Fragments:	Don't Care 👻	
Application	Action/Profile	Syslog
Filter:	Block Immediately -	
Branch to Other Filter Set:	None 🔻	
IM/P2P Filter:	None 👻	
URL Content Filter	None 👻	
Web Content Filter	None 💌	
Advance Setting	Edit	

Screenshot 52 - DrayTek: Edit Filter Rule view (IP addresses greater than the GFI WebMonitor proxy machine IP address)

# 6.7.6 Linksys WRT54GL Wireless Router

On Linksys WRT54GL Wireless Router, ports are not blocked directly; they are blocked by creating internet access restrictions. To create a restriction to block HTTP on port 80:

- 1. Open the web configuration page from an internet browser.
- 2. Provide any credentials required.

LINKSYS® A Division of Cisco Systems, Inc.		Firmware Version : v4.30.7
Access	Wireless-G Broad	lband Router WRT54GL
Restrictions	Setup         Wireless         Security         Access Restrictions         Applications           Internet Access         Acces	Administration Status
Internet Access Blocked Services	Internet Access       1 ()       Delete       Summary         Status :	Internet Access Policy : You may define up to 10 access policies. Click Delete to delete a policy or Summary to see a summary of the policy. Status : Enable or disable a policy. Policy Name : You may assign a name to your policy. Policy Type : Choose from Internet Access or Inbound Traffic. More Days : Choose the day of the week you would like your policy to be applied. Times : Enter the time of the day you would like your policy to apply. Blocked Services : You may choose to block access to certain services. Click Add/Edit Services to modify these settings. Website Blocking by URL : You can block access to certain unbock access to certain
Website Blocking by URL Address		Website Blocking by Keyword: You can block access to certain website by the keywords contained in their webpage.

Screenshot 53 - Linksys WRT54GL Wireless Router: Internet Access view

3. From the router's configuration web interface, click Access Restrictions tab ► Internet Access.

- 4. From the Internet Access Policy drop-down list, select a number.
- 5. From the Status radio buttons, select Disable. (Select Enable to start blocking immediately).
- 6. In the Enter Policy Name text box, key in a name.
- 7. Click Edit List of PCs button.

	List o	of PCs		
Ent	er MAC Address of the PC:	s in this format :	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	
MAC 01 :	00:00:00:00:00:00	MAC 05 :	00:00:00:00:00:00	
MAC 02:	00:00:00:00:00:00	MAC 06 :	00:00:00:00:00:00	
MAC 03 :	00:00:00:00:00:00	MAC 07 :	00:00:00:00:00:00	
MAC 04 :	00:00:00:00:00:00	MAC 08:	00:00:00:00:00:00	
	Enter the IP Add	dress of the PC:	5	
IP	<b>01:</b> 192.168.1. 0	IP 04 : 19	2.168.1. 0	
IP	<b>02:</b> 192.168.1. 0	IP 05 : 19	2.168.1. 0	
IP	03: 192.168.1. 0	IP 06 : 19	02.168.1. 0	
	Enter the IP Ra	ange of the PCs		
P Range 01 :	192.168.1. 1 ~ 100	IP Range 02	2: 192.168.1. 102 ~ 254	
	Save Settings	Cancel	Changes	

Screenshot 54 - Linksys WRT54GL Wireless Router: List of PCs dialog

8. In **IP Range 01** text boxes, key in the IP addresses of the range of IP addresses smaller than the GFI WebMonitor proxy machine IP address (excluding the proxy machine's IP address).

9. In **IP Range 02** text boxes, key in the IP addresses of the range of IP addresses greater than the GFI WebMonitor proxy machine IP address (excluding the proxy machine's IP address).

- 10. Click Save Settings button.
- 11. From the **PCs** radio buttons, select **Deny**.

12. From the **Blocked Services** first drop-down list, select **HTTP** and key in "80" and "80" respectively.

- 13. (Optional) Click Add/Edit Service to create or modify a service.
- 14. Click Save Settings.

# 6.7.7 Thomson Wireless Broadband Router TG585 v7

On **Thompson Wireless Broadband Router TG585 v7**, ports are blocked by creating firewall access rules. This section describes how to:

- » Create a firewall access rule to allow Web (HTTP) traffic originating from GFI WebMonitor Proxy machine
- » Create a firewall access rule to block all outgoing HTTP traffic

# Step 1: Creating a Firewall Access Rule to Allow HTTP Traffic From GFI WebMonitor Proxy

To create a firewall access rule to allow Web (HTTP) traffic originating from GFI WebMonitor Proxy machine:

- 1. Open the web configuration page from an internet browser.
- 2. Provide any credentials required.

	Home > Toolbo	<u>x</u> > <u>Firewall</u> > <u>Ne</u>	entry2				Overvie	w   <u>Configu</u>
Home	alle >	New_entr	y2					
	552	<ul> <li>Firewall</li> </ul>	Settings					
Thomson Gateway		Select a ro	w using the 'E	dit' link b	o modify a rule.			
Contractory of the second s		Click Add	to add a firewa	all rule.				
Broadband Connection		Enable	Name	Action	Source Intf/Ip	Destination Intf/Ip	Service	Hits
Toolbox		X1		V	1		htte	-
mote Assistance		N.	allow		lan	АЛУ	netp	2.4
me & Application Sharing					192.168.1.101	Any		
rewall		11	-	X	in a			
trusion Detection		V	BlockWWW	^	lan	wan	http	96
mamic DNS								
an Management								

Screenshot 55 - Thompson Wireless Broadband Router TG585 v7: Firewall Settings view

- 3. From the router's configuration web interface, click **Toolbox > Firewall**.
- 4. From the Firewall Settings, select Configure.
- 5. Click Add button to add a new firewall rule.

14	Firewall Rule		
2013	<ul> <li>Rule Definition</li> </ul>		5
	Name:	allow	
	Enabled:		
	Source Interface:	lan	
	Source Address:	192.168.1.101	•
	User-Defined:		
	Destination Interface:	Any	
	Destination Address:	Any	
	User-Defined:		
	Service:	http	•
	Action:	Accept	
		A	pply Cancel

 $\label{eq:screenshot} \textit{Screenshot 56-Thompson Wireless Broadband Router TG585 v7: Firewall Rule view}$ 

- 6. Key in a name in the Name text box, for example "allow".
- 7. Check Enabled checkbox.
- 8. From the Source Interface drop-down list, select lan.
- 9. To specify the IP address of the GFI WebMonitor proxy machine:

- » Option 1: From the Source Address drop-down list, select the IP address of the GFI WebMonitor proxy machine.
- » Option 2: In the User-Defined text box, key in the IP address of the GFI WebMonitor proxy machine
- 10. From the **Destination Interface** drop-down list, select **Any**.
- 11. From the **Destination Address** drop-down list, select **Any**.
- 12. From the **Service** drop-down list, select **HTTP**.
- 13. From the Action drop-down list, select Accept.
- 14. Click Apply to save settings.

# Step 2: Creating a Firewall Access Rule to Block All Outgoing HTTP Traffic

To create a firewall access rule to block all Web (HTTP) traffic:

- 1. Open the web configuration page from an internet browser.
- 2. Provide any credentials required.
- 3. From the router's configuration web interface, click **Toolbox > Firewall**.
- 4. From the Firewall Settings, select Configure.
- 5. Click Add button to add a new firewall rule.

1 B 6	<ul> <li>Rule Definition</li> </ul>		
	Name:	BlockWWW	
	Enabled:		
	Source Interface:	lan	
	Source Address:	Any	
	User-Defined:		
	Destination Interface:	wan	•
	Destination Address:	Any	-
	User-Defined:		
	Service:	http	•
	Action:	Deny	•

Screenshot 57 - Thompson Wireless Broadband Router TG585 v7: Firewall Rule view

- 6. Key in a name in the Name text box, for example "BlockWWW".
- 7. Check Enabled checkbox.
- 8. From the Source Interface drop-down list, select lan.
- 9. From the Source Address drop-down list, select Any.
- 10. From the **Destination Interface** drop-down list, select **wan**.
- 11. From the Destination Address drop-down list, select Any.

- 12. From the Service drop-down list, select HTTP.
- 13. From the Action drop-down list, select Deny.
- 14. Click **Apply** to save settings.

# 6.8 Disabling Internet Connections Settings on Client Machines

To prevent users from modifying Internet settings and thus bypassing GFI WebMonitor, the Internet **Connections** settings tab can be disabled on client machines.

# 6.8.1 Disabling Internet Connections Page Using GPO in Microsoft Windows Server 2003

To disable **Connections** settings on client 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**.

masterdomain.co	m Properties			? ×
General Manage	ed By Group Policy			
To improve Grou Management Co	ip Policy manageme nsole (GPMC).	nt, upgrade	to the Group Po	blicy
Curr	ent Group Policy Ob	ject Links fo	r masterdomain	
Group Policy 0	bject Links nain Policy		No Override	Disabled
I Group Policy Ob This list obtained	jects higher in the lis I from: win2k3serv.m	t have the h hasterdomain	ighest priority. com	
New	A <u>d</u> d	<u>E</u> dit		<u>Ш</u> р
Options	Dele <u>t</u> e	<u>P</u> roperties		Do <u>w</u> n
□ <u>B</u> lock Policy	inheritance			
	0	ĸ	Cancel	Apply

Screenshot 58 - 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.



Screenshot 59 - GPO Editor window

5. Expand User Configuration ► Administrative Templates ► Windows Components ► Internet Explorer and click Internet Control Panel.

6. Right-click **Disable the Connections page** from the right panel and click **Properties**.

Disable the Connections page Properties	? ×
Setting Explain	
Disable the Connections page	
C Not <u>C</u> onfigured	
€ Enabled	
C <u>D</u> isabled	
Supported on: at least Internet Explorer v5.0	
Previous Setting <u>N</u> ext Setting	
OK Cancel App	dy.

Screenshot 60 - Disable the Connection page Properties dialog

#### 7. In the **Setting** tab, select **Enabled**.



- 8. Click Apply and OK.
- 9. Close all open windows.

# 6.8.2 Disabling Internet Connections Page Using GPO in Microsoft Windows Server 2008

To disable **Connections** settings on clients' 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.

nap-in	Vendor 🔺		Console Root		Edit Extensions
Device Manager	Microsoft (		📕 Group Policy Ma	anagement	2
Disk Management	Microsoft				Remove
DNS	Microsoft				
Event Viewer	Microsoft				Move Up
Exchange Server 2007	Microsoft				,
Folder	Microsoft 🦳				Move Down
Group Policy Management	Microsoft	Add >			
Group Policy Management E	Microsoft				
Group Policy Object Editor	Microsoft				
Group Policy Starter GPO Ed	Microsoft				
Internet Information Servic	Microsoft				
Internet Information Servic					
IP Security Monitor	Microsoft 💶				Advanced
			<u> </u>		Advanced
rintion:					
ciptori					

Screenshot 61 - Add/Remove Snap-ins window

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

4. Click OK.



Screenshot 62 - Console Root domain window

# 5. Expand Group Policy Management Forest Domains and <domain>.

6. Right-click **Default Domain Policy** and click **Edit** to open the **Group Policy Management Editor**.



Screenshot 63 - Group Policy Management Editor window

7. Expand User Configuration ► Policies ► Administrative Templates ► Windows Components ► Internet Explorer and click Internet Control Panel.

8. Right-click **Disable the Connection page** from the right panel and click **Properties**.

Disable the Connections page Properties	? ×
Setting Explain Comment	
Disable the Connections page	
Not Configured	
Enabled	
C Disabled	
Supported on: At least Internet Explorer 5.0	
Previous Setting Next Setting	
OK Cancel Apply	,

Screenshot 64 - Disable the Connection page Properties dialog

9. In the **Setting** tab, select **Enabled**.



This policy prevents users from viewing and modifying connection and proxy settings from their client machines.

- 10. Click Apply and OK.
- 11. Close Group Policy Management Editor dialog and save the management console created.

#### 6.9 Assigning Log On As A Service Rights

# 6.9.1 Assigning Log On As A Service Rights on Microsoft Windows XP, Microsoft Windows Vista and Microsoft Windows 7 Manually

To assign **Log on as a service** rights to a user account on Microsoft Windows XP (SP2) or Microsoft Windows Vista machine manually:

- 1. Navigate to **Start ► Control Panel ► Administrative Tools ► Local Security Policy**.
- 2. Expand Security Settings ► Local Policies ► User Rights Assignment.
- 3. Right-click Log on as a service from the right panel and click Properties.
- 4. Select the Local Security Setting tab.
- 5. Click Add User or Group button.
- 6. Key in the account name and click **OK**.
- 7. Click **Apply** and **OK**.
- 8. Close Local Security Settings dialog.
- 9. Close all open windows.

#### 6.9.2 Assigning Log On As A Service Rights on a Server Machine Manually

To assign **Log on as service** rights to a user account on Microsoft Windows Server 2003 or Microsoft Windows Server 2008 machines manually:

1. Navigate to **Start** ► **Programs** ► **Administrative Tools** ► **Local Security Policy**.

http://www.com/com/com/com/com/com/com/com/com/com/			_ 🗆 🗡
File Action View Help			
🗢 🔿 🖄 📷 💥 🗎 🗟 📘			
Security Settings	Policy 🔺	Security Setting	<b></b>
🕀 🧾 Account Policies	Impersonate a client after authen	LOCAL SERVICE, NE	
🖃 📴 Local Policies	Increase a process working set	Users	
E Audit Policy	Increase scheduling priority	Administrators	
Security Options	Load and unload device drivers	Administrators	
End Security Options End Security options	Lock pages in memory		
Network List Manager Policies	Log on as a batch job	Administrators,Back	
	End on as a service	Administrator	
	Manage auditing and security log	Administrators	
🗉 展 IP Security Policies on Local Computer	Modify an object label		
	Modify firmware environment values	Administrators	
	Perform volume maintenance tasks	Administrators	
	Profile single process	Administrators	
	Profile system performance	Administrators	
	Remove computer from docking st	Administrators	
	Replace a process level token	LOCAL SERVICE, NE	
	Restore files and directories	Administrators,Back	]
۲	Shut down the system	Administrators,Back	-

Screenshot 65 - Microsoft Windows Server: Local Security Policy window

# 2. Expand Security Settings ► Local Policies ► User Rights Assignment.

- 3. Right-click Log on as a service from the right panel and click Properties.
- 4. Select the Local Security Setting tab.
- 5. Click Add User or Group button.
- 6. Key in the account name and click **OK**.
- 7. Click Apply and OK.
- 8. Close all open windows.

# 6.9.3 Assigning Log On As A Service Rights Using GPO in Microsoft Windows Server 2003

To assign Log on as service rights on clients' 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**.

masterdomain.com Properties	? ×
General Managed By Group Policy	
To improve Group Policy management, upgrade to the Gro Management Console (GPMC).	oup Policy
Current Group Policy Object Links for masterd	omain
Group Policy Object Links No Ove S Default Domain Policy	rride Disabled
, Group Policy Objects higher in the list have the highest pri This list obtained from: win2k3serv.masterdomain.com	ority.
New     Add     Edit       Options     Delete     Properties	Up Do <u>w</u> n
□ <u>B</u> lock Policy inheritance	
OK Cancel	Apply

Screenshot 66 - 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**

🚡 Group Policy Object Editor		
<u>File Action View Help</u>		
🛐 Default Domain Policy [win2k3serv.masterdomain 🔺	Policy 🛆	Policy Setting
📄 👼 Computer Configuration 👘 👘	BDeny log on through Terminal Services	Not Defined
🗄 💼 Software Settings	Enable computer and user accounts to be tr	Not Defined
📄 🖳 Windows Settings	BForce shutdown from a remote system	Not Defined
Scripts (Startup/Shutdown)	Generate security audits	Not Defined
E Security Settings	Impersonate a client after authentication	Not Defined
	Increase scheduling priority	Not Defined
Cocal Policies	BLoad and unload device drivers	Not Defined
	Buck pages in memory	Not Defined
E Security Options	Bellog on as a batch job	Not Defined
Event Log	🔢 Log on as a service	MASTERDOMAIN\Admin
	📖 Manage auditing and security log	Not Defined
	Modify firmware environment values	Not Defined
	Berform volume maintenance tasks	Not Defined
🕀 🧰 File System	Profile single process	Not Defined
⊕      ₩ Wireless Network (IEEE 802.11) F	Profile system performance	Not Defined
🕀 💼 Public Key Policies	Remove computer from docking station	Not Defined
😥 💼 Software Restriction Policies	😥 Replace a process level token	Not Defined
🕀 🛃 IP Security Policies on Active Dire	Restore files and directories	Not Defined
i Administrative Templates	避 Shut down the system	Not Defined
E 🕵 User Configuration	👿 Synchronize directory service data	Not Defined
E I Software Settings	避 Take ownership of files or other objects	Not Defined
Windows Settings		

Screenshot 67 - GPO Editor window

5. Expand Computer Configuration ► Windows Settings ► Security Settings ► Local Policies and click User Rights Assignment.

6. Right-click Log on as a service from the right panel and click Properties.

- 7. Select the Security Policy Setting tab.
- 8. Check **Define these policy settings** checkbox
- 9. Click Add User or Group button.
- 10. Key in the account name and click **OK**.
- 11. Click Apply and OK.
- 12. Close all open windows.

# 6.9.4 Assigning Log On As A Service Rights Using GPO in Microsoft Windows Server 2008

To assign **Log on as service** rights on clients' 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.

ap-in	Vendor 🔺		Console Root		Edit Extensions
Device Manager	Microsoft		Group Policy Ma	nagement	
Disk Management	Microsoft ;				Remove
DNS	Microsoft (				
Event Viewer	Microsoft				Move Lip
Exchange Server 2007	Microsoft				40.0101
Folder	Microsoft 🦳				Move Down
Group Policy Management	Microsoft	Add >			
Group Policy Management E	Microsoft				
Group Policy Object Editor	Microsoft				
Group Policy Starter GPO Ed	Microsoft (				
Internet Information Servic	Microsoft (				
Internet Information Servic					
IP Security Monitor	Microsoft 🔼				Advanced
			<u> </u>		Advanced
rintion:					
- Provint					

Screenshot 68 - Add/Remove Snap-ins window

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

🚟 Console1 - [Console Root\Group Policy I	lanagement\Forest: techcom.com\Domains\techcom.com ]
🚟 File Action View Favorites Window	Help
🗢 🔿 🙍 🖬 📋 🗔 🧟 🔽 🖬	
Console Root	techcom.com
☐ I Group Policy Management ☐ A Forest: techcom.com	Linked Group Policy Objects Group Policy Inheritance Delegation
🖃 🚰 Domains	Link Order 🔺 GPO Enforced Link Enabled GPO
E 📰 techcom.com	🚖 1 🚮 Default Domain Policy No Yes Enab
Default Domain Policy	
Domain Controllers	
🛨 🧧 Microsoft Exchange Secu	
Group Policy Objects	
E Starter CPOs	$\Xi$
	]

Screenshot 69 - Console Root domain window

# 5. Expand Group Policy Management ► Forest ► Domains and <domain>.

6. Right-click **Default Domain Policy** and click **Edit** to open the **Group Policy Management Editor**.

Group Policy Management Editor		
File Action View Help		
🗢 🔿 🙍 🕱 🖺 🔒 🛛 🖬		
Default Domain Policy [TECHCOM02.TECHCOM.COM] Policy	Policy 🔺	Policy Setting
E 🛃 Computer Configuration	Deny log on as a service	Not Defined
	Deny log on locally	Not Defined
⊕ Software Settings     □	Deny log on through Terminal Services	Not Defined
Windows Settings	Enable computer and user accounts to be tr	Not Defined
Scripts (Startup/Shutdown)	Force shutdown from a remote system	Not Defined
E Security Settings	Generate security audits	Not Defined
Account Policies	Impersonate a client after authentication	Not Defined
	Increase a process working set	Not Defined
	Increase scheduling priority	Not Defined
	Load and unload device drivers	Not Defined
E Fvent Log	Lock pages in memory	Not Defined
Restricted Groups	Log on as a batch job	Not Defined
T System Services	🐻 Log on as a service	Not Defined
Registry	Manage auditing and security log	Not Defined
🕀 🔂 File System	Modify an object label	Not Defined
🕀 🧑 Wired Network (IEEE 802.3) Policies	Modify firmware environment values	Not Defined
🗉 🧮 Windows Firewall with Advanced Security	Perform volume maintenance tasks	Not Defined
Network List Manager Policies	Profile single process	Not Defined
🛨 🚂 Wireless Network (IEEE 802.11) Policies	Profile system performance	Not Defined
🗉 📔 Public Key Policies	Remove computer from docking station	Not Defined
E Software Restriction Policies	Replace a process level token	Not Defined
Image: Second S	Restore files and directories	Not Defined
IP Security Policies on Active Directory (TL	Shut down the system	Not Defined
Policy-based QoS	Synchronize directory service data	Not Defined
Administrative Templates: Policy definitions (ADM:	Take ownership of files or other objects	Not Defined
Preferences		· · · · · · · · · · · · · · · · · · ·
	•	Þ

Screenshot 70 - Group Policy Management Editor window

7. Expand Computer Configuration ► Policies ► Windows Settings ► Security Settings ► Local Policies and click User Rights Assignment.

- 8. Right-click Log on as a service from the right panel and click Properties.
- 9. Select the Security Policy Setting tab.
- 10. Check Define these policy settings checkbox
- 11. Click Add User or Group button.

- 12. Key in the account name and click **OK**.
- 13. Click Apply and OK.
- 14. Close all open windows.

# 6.10 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 71 - 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**.

masterdomain.com Properties	? ×			
General Managed By Group Policy				
To improve Group Policy management <u>upgrade</u> to the Group Policy Management Console (GPMC).				
Current Group Policy Object Links for masterdomain				
Group Policy Object Links No Override Disabled				
, Group Policy Objects higher in the list have the highest priority. This list obtained from: win2k3serv.masterdomain.com				
<u>N</u> ew A <u>d</u> d <u>E</u> dit <u>⊔</u> p				
Options Delete Properties Down				
□ <u>B</u> lock Policy inheritance				
OK Cancel Apply	,			

Screenshot 72 - 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.

oft (		Console Root	Management	Edit Extensions
oft; oft; oft; oft; oft;		E Group Policy	Management	Remove
oft; oft; oft; oft;				Remove
oft ( oft ( oft (				
oft ( oft (				
oft				Move Up
oft (	Add >			Move Down
oft	Auu /			
ioft (				
oft (				
oft (				
soft (				
				Advanced
		1		
	soft ( soft ( soft ( soft ( soft ( ▶	soft i Add > soft i soft i soft i soft i soft i	soft (	soft (

Screenshot 73 - Add/Remove Snap-ins window

#### 3. Select Group Policy Management from the Available snap-ins list, and click Add.

4. Click OK.

🚟 Console1 - [Console Root\Group Policy	fanagement\Forest: techcom.com\Domains\techcom.com ]
🚡 File Action View Favorites Window	Help
Console Root	techcom.com
Group Policy Management     A Forest: techcom.com	Linked Group Policy Objects Group Policy Inheritance Delegation
🖃 🙀 Domains	Link Order 🔺 GPO Enforced Link Enabled GPO
E P Techcom.com	1 🚮 Default Domain Policy No Yes Enab
WMI Filters      Starter CPOs	*

Screenshot 74 - Console Root domain window

5. Expand Group Policy Management ► Forest ► Domains and <domain>.

6. Right-click **Default Domain Policy** and click **Edit** to open 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

## 7 Troubleshooting

#### 7.1 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

#### 7.2 Common Issues

ISSUE ENCOUNTERED	
Users are not able to browse and/or download from the Internet after installing GFI WebMonitor in Gateway or in Simple Proxy mode.	After the installation, GFI WebMonitor proxy machine has to be configured to listen for incoming user requests. For more information, refer to the Administration and Configuration manual. Next, Internet browsers on client machines have to be configured to use the GFI WebMonitor proxy machine as the default proxy. For more information, refer to the Post-installation Actions section in the Installing in Gateway mode chapter or refer to the Post-installation Actions section in the Installing in Simple Proxy mode chapter as applicable. 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. For more information on how to enable firewall ports on Microsoft Windows Firewall, refer to http://kbase.gfi.com/showarticle.asp?id=KBID003879
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 <b>Refresh cached Internet Explorer</b> <b>settings</b> section within the <b>Miscellaneous</b> chapter in GFI WebMonitor <b>Getting Started Guide</b> . 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 <b>Guest only - local users authenticate as Guest.</b> For more information, refer to the Configuring Network Access Policy section in the Miscellaneous chapter.

ISSUE ENCOUNTERED	SOLUTION
Users using Mozilla Firefox browsers are repeatedly asked to key in credentials after installing GFI WebMonitor in Gateway or in Simple Proxy mode	The server and the client machine will use NTLMv2 for authentication when: GFI WebMonitor is installed on Microsoft Windows Server 2008 and LAN Manager authentication security policy is defined as Send NTLMv2 response only
mode.	and
	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 GEI 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

### 7.3 Knowledge Base

GFI maintains a comprehensive Knowledge Base repository that includes answers to the most common problems. In case that the information in this manual does not solve your installation problems, next refer to the Knowledge Base. The Knowledge Base always has the most up-to-date listing of technical support questions and patches. Access the Knowledge Base by visiting: http://kbase.gfi.com/.

### 7.4 Web Forum

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

#### 7.5 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 visit http://www.gfi.com/company/contact.htm.



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

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

#### 7.6 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.

# 8 Glossary

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

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

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

## Index

### A

Access Control 75 Active Directory GPO 14, 58, 67, 72 Anti-virus 2, 77

## В

Bandwidth 75 Build Notifications 73

### С

Cache 40, 75 Chained Proxy 40, 41 Cisco ADSL Router Cisco 47 Console 13, 16, 30, 37, 38, 42, 44, 47, 60, 62, 66, 69, 75

### D

Dashboard 37 DrayTek VIGOR 49

### Н

Hidden downloads 75

#### I

Integrated authentication 67, 71 Internet Gateway 6, 9, 10

#### L

License key 11, 25, 39 Linksys 53, 54 Log on as a service rights 26, 62, 63

#### M

Malware 6 MSN 76 Netgear Wireless Router 47, 48

## Ρ

Ν

Phishing 1, 6
Port Blocking 7, 42
Proxy Server 7, 13, 15, 17, 18, 20, 22, 23, 27, 29, 31, 32, 34, 36, 41, 75

### R

Reporting 9, 23

#### S

Simple Proxy 1, 23, 27, 42, 72 Snap-ins 15, 16, 30, 60, 65, 69 SonicWall 42, 44, 45, 46 Spyware 1, 6

### Т

Technical Support 72, 73 Temporary Whitelist 6 Thomson 55 Traffic Forwarding 7, 8, 24, 42, 76

### U

Unified Protection Edition 2, 6 User Agent 77

### W

Web Forum 73 Web traffic 1, 2, 5, 6, 40, 41, 77 WebFilter Edition 2, 6, 37 WebGrade Database 2, 5 WebSecurity Edition 2, 6, 37

#### USA, CANADA AND CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104, Cary, NC 27513, USA Telephone: +1 (888) 243-4329 Fax: +1 (919) 379-3402 Email: ussales@gfi.com

#### UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines, Middlesex, TW18 4BP, UK Telephone: +44 (0) 870 770 5370 Fax: +44 (0) 870 770 5377 Email: sales@gfi.co.uk

#### EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta Telephone: +356 2205 2000 Fax: +356 2138 2419 Email: sales@gfi.com

#### AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia Telephone: +61 8 8273 3000 Fax: +61 8 8273 3099 Email: sales@gfiap.com



#### Disclaimer

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

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