GFI WebMonitor™

Web security, monitoring and Internet access control

Smart Guide for GFI WebMonitor for ISA/TMG

GFI®

Welcome to GFI WebMonitor™ for ISA/TMG (WebMonitor): This solution gives you complete control, in real time, to monitor what users are browsing on the Internet and/or to ensure that any files they download are free of viruses and other malware.

Introduction

This SmartGuide is an important tool to enhance your success with the product. This SmartGuide includes the following:

1. **GFI WebMonitor Product Overview**
2. **Why Customers Purchase WebMonitor**
3. **Which GFI WebMonitor Edition is right for my Organization?**
4. **Five (5) Major Points to Consider Before Deploying WebMonitor**

GFI WebMonitor is easy to install and get running; however, there are items that need to be understood before installing it. From our experience, if these items are not addressed, there could be situations where configuration issues could impact the performance of the product and, therefore, your success with it.

GFI WebMonitor offers two installation modes.

1. **The standard installation**
2. **A special installation for** the unique needs of **Microsoft's Internet Security and Acceleration (ISA) Server and Threat Management Gateway Server (TMG) - WebMonitor for ISA/TMG.**

This SmartGuide is for GFI WebMonitor ISA/TMG.

Through this Guide and a little planning ahead of time, you will be able to deploy an efficient and easy-to-maintain environment. Please take the time to review this document before installing the product.
For additional detailed documentation you can reference GFI's Knowledge Base, (**kbase.gfi.com**) and the GFI WebMonitor documentation located **here**.

If, after reading the SmartGuide, you have questions about any of the issues raised in this document, please contact our support organization at **www.gfi.com/company/contact.htm** or electronically at **support.gfi.com/Support/supportrequest.aspx?lcode=en**.

GFI WebMonitor overview

Let's start with a review of what GFI WebMonitor does. Simply stated:

1. It **provides visibility into**:
   - **what web sites your users are browsing**,
   - **how much time they are spending on the Internet**,
   - the amount of bandwidth being consumed, and more.
2. It **allows you to define web filtering and web browsing policies** to help enforce an effective Internet Usage Policy.
3. Its web security features allow you to **control, monitor and block what type of files users can download** on a per user or per IP basis.

Why do customers purchase GFI WebMonitor?

Based on our experience, below are the top four (4) reasons GFI customers purchase GFI WebMonitor:

1. To **monitor, manage and enforce users' use of the Inte**rnet in order to enforce the company's Internet Usage Policy.
2. To **manage which types of files users can download** from the Internet.

3. To **protect the organization from dangerous viruses due to downloads** from the Internet and protect them from Phishing websites.
4. To meet legal and/or compliance requirements* by protecting your system resources and securing your confidential data from malware/spyware viruses and protecting users from doing illegal downloads or illicit website access.

* **Note**: Without the ability to exercise some form of management over what your users are browsing, you leave your organization open to legal liability in a variety of ways.

Which GFI WebMonitor edition is right for my organization?

Before you choose which Edition of GFI WebMonitor to license, it is important to understand the requirements for your company's ***Internet Usage Policy***. An Internet Usage Policy is the business policies and practices that you would like to enforce on your network. See **Sample Internet Usage Policy**.

At a basic level there are two types of Internet usage policies:

1. To increase the employee's productivity by **controlling access to unproductive sites**.
2. **To control downloads** and **reduce the risks** and threats associated with viruses/malware and other potential problems associated with the types of files employees will download.

GFI WebMonitor is available in three (3) different Editions:

1. The **WebFilter Edition** includes a dynamic database of 250,000,000+ urls. These websites are categorized based on the content of the website. You decide to ALLOW, BLOCK OR QUARANTINE the category or the site. You can also decide to give limited access to sites / categories (e.g. 1 hour per day, or 100Mb per week).
2. The **WebSecurity Edition**, using multiple anti-virus engines, protects you organization from viruses, malware/spyware and phishing websites by scanning each download before allowing the download.
3. The Unified **Protection Edition is a combination of both the WebFilter and the WebSecurity Editions**. This is the most comprehensive web monitoring solution providing both content filtering and protection against security threats. The Unified Protection Edition is generally used when companies are implementing a total web-use policy. This edition allows you to implement the ideal Internet monitoring and access control solution.

Business Needs met by GFI Webmonitor

Business needs	WebFilter	WebSecurity	Unified Protection
General Features			
Supports Windows Workgroups	✓	✓	✓
Active Directory Integration (Users & Groups)	✓	✓	✓
HTTP/FTP Protocol Filtering	✓	✓	✓
HTTPS Protocol Filtering	✓*	✓	✓*
User/IP/Site Black & White List	✓	✓	✓
Proxy Caching	✓	✓	✓
Administration			
Retention of User Browsing History	✓	✓	✓
Quarantine	✓	✓	✓
Quarantine Approval & Deletion	✓	✓	✓
Real Time Monitoring			
Connection Monitoring (active & past)	✓	✓	✓

Business needs	WebFilter	WebSecurity	Unified Protection
User & Site History Monitoring	✓	✓	✓
Bandwidth Monitoring	✓	✗	✓
Web Filtering			
User/Group-based URL Categorization	✓	✗	✓
User/Group/IP Web Filtering Policies	✓	✗	✓
Time-based Web Filtering Policies	✓	✗	✓
User/Group/IP Time Based Thresholds	✓	✗	✓
User/Group/IP Bandwidth Based Thresholds	✓	✗	✓
Content & Antivirus			
Download Control Policies	✗	✓	✓
True File Type Checking	✗	✓	✓
Control Compressed Archive (Zipped) files	✗	✓	✓
Multiple Antivirus Engines	✗	✓	✓
User/Group/IP-based Virus Scanning Policies	✗	✓	✓
Protection from Malware, Spyware & Greyware	✗	✓	✓
Heuristic Scanning & Macros	✗	✓	✓
Anti-Phishing	✗	✓	✓

** Requires you to configure GFI WebMonitor to decrypt https traffic for scanning. For more information, go* ***here.***

Determining the correct Edition for your company can be simplified by answering a question about your company's goals for an Internet Usage Policy.

Are you concerned with?

1. Increasing employee productivity **OR**
2. Reducing the risks and threats to your network **OR**
3. Both?

If you answered:

- **Productivity only**, then the **WebFiltering Edition** is right for you.
- **Reducing Threats**, then the **WebSecurity Edition** is right for you.
- **Both**, then the **Unified Protection Edition** is right for you.

If you are unsure exactly which edition is the best fit for your company, please **contact us**.

Before deploying GFI WebMonitor

There are six (6) major aspects to consider before deploying GFI WebMonitor. It is important that you understand each of these. If after reading the sections below, you have any questions or want to discuss any of them further, please **contact us**.

1. **Licensing GFI WebMonitor**
2. **System Installation Requirements**
3. **Authentication**
4. **Configuring Client Web Browsers**
5. **Enforcing your Internet Usage Policy**
6. **Reporting**

1. Licensing GFI WebMonitor: Determining License Count

A GFI WebMonitor unit is a seat. A seat is defined as either an IP address or user depending on whether the connection being processed by GFI WebMonitor has been "***authenticated***" or "**not authenticated**":

- A **seat is defined as a user** when there is an authenticated connection. Where GFI WebMonitor records the username of the user making the connection.
- A **seat is defined as an IP address** for unauthenticated connections. Where GFI WebMonitor records the IP address of the computer making the connection.

It is important to understand how a license is counted: **should the use count exceed the licensed count** (paid licenses), **all additional users/IPs** above the license limit **are NOT protected by GFI WebMonitor**.

There are situations where authenticated and unauthenticated connections are performed within the same network. In such cases, licensing is determined as follows:

Connections	Number of Licenses
Authenticated and unauthenticated connection made from the same machine	1
Authenticated user making two (2) connections from different machines (thus different IPs)	1
Connections from whitelisted IP addresses	0
Two (2) authenticated users making connection from the same machine	2

Users can be whitelisted; however, if a service account making use of authentication connects to the Internet, this will be counted as another licensed user. This is why it is recommended to whitelist IPs instead of users to ensure that traffic on that machine is whitelisted.

2. System Installation Requirements

The installation requirement for GFI WebMonitor depends on the Edition. Below are minimum requirements to use and install GFI WebMonitor.

GFI WebMonitor **WebMonitor** Hardware Requirements

	Minimum Hardware Requirements on Edition		
Edition	**Processor**	**RAM**	**Hard Disk**
WebFilter	2.0 GHz	1 GB*	2 GB of available disk space
WebSecurity	2.0 GHz	1 GB*	10 GB of available disk space
Unified Protection	2.0 GHz	2 GB*	12 GB of available disk space

**4 GB of RAM is recommended for best performance.*

GFI WebMonitor for ISA/TMG Software Requirements

Supported Operating Systems	Other Required/Recommended Components
Microsoft Windows Server 2000 (SP4) Microsoft Windows Server 2003 (x86) Microsoft Windows Server 2008 R2(x64)	Microsoft ISA Server 2004 (SP3) Microsoft ISA Server 2006 Microsoft Forefront TMG 2010 (Microsoft Windows Server 2008 R2) Microsoft Internet Explorer 6 or later Microsoft.NET framework 2.0 TCP/IP port 1007 Microsoft SQL Server 2000 or later (for reporting purposes) (Recommended) Microsoft Firewall Client for ISA Server (Recommended) Microsoft Firewall Client for Microsoft Forefront TMG

For GFI WebMonitor ISA Server/Forefront TMG installations with more than 500 seats there are several Microsoft "Best Practices Guides". For ISA/TMG installations, we strongly suggest you read them. Click **here** to access these Guides.

3. Authentication

GFI WebMonitor for ISA/TMG, ISA/TMG must be configured to enforce authentication.

- GFI WebMonitor gets the IP and username (if authenticated) directly from Microsoft ISA/TMG
- If Microsoft ISA/TMG logs the username in its proxy log, GFI WebMonitor will have access to the username.

For more information, go **here**.

4. Configuring Client Web Browsers

GFI WebMonitor for ISA/TMG - Configuring Client Web Browsers

GFI WebMonitor for ISA/TMG **requires that you configure the client's/user's web browser** to make use of the ISA/TMG server on which GFI WebMonitor is installed as the proxy server for web traffic requests. This is how the product ensures that all users are being filtered. To do this you can:

1. Manually configure the user's web browser to point to the machine on which GFI WebMonitor is installed as the proxy server, or
2. Use Group Policy to configure the web browsers automatically*
3. Use ISA/TMG clients to configure the web browsers automatically.

If you are going to apply policies to users/groups, you MUST set your ISA/TMG server to REQUIRE authenticated connections. If you don't set your ISA/TMG server to require authenticated connections, policies created for users/groups will not be applied. More details on how to configure authenticated connections can be found **here**.

*If you are going to apply policies to users/groups, you MUST set your ISA/TMG server to REQUIRE authenticated connections. If you don't set your ISA/TMG server to require authenticated connections, policies created for users/groups will not be applied. More details on how to configure authenticated connections can be found **here**.

5. Enforcing your Internet Usage Policy in GFI WebMonitor

GFI WebMonitor makes use of two types of policies to enforce Internet Usage Policy based on your company needs. These policies can be applied "all inclusive" to all IPs, all users, all groups, etc.; or as granular as to specific IPs, users, or groups. Policies can be enforced during specific hours, or remain on continuously.

- **WebFiltering Policies**, found in the WebFiltering Edition of the product, allows you to control internet access to categories of websites.
- **Web Browsing Policies**, found in the WebFiltering Edition of the product, allows you to control browsing time and download bandwidth thresholds instead of only blocking a web site.
- **Download Control Policies**, found in the WebSecurity Edition of the product, allows you to create policies per user(s), group(s) and/or IP(s) to manage file downloads based on file types. Download control policies are aimed at the "bad things" such as viruses, malware and phishing sites and can control file types that are often very large from being downloaded. This can help reduce the need for additional storage and the associated costs and keeps inappropriate data from being backed up.

Once you create the policy, then you decide what actions should be taken. The product provides for three (3) actions that you can take on a policy; **ALLOW, QUARANTINE or BLOCK**.

- ALLOW is used in cases where a policy has been created to ensure that specific traffic is always accessible.
- QUARANTINE is used when potential traffic may be harmful, the quarantine can be used to temporarily hold the site so that it can be reviewed and either Allowed or Blocked by the IT Administrator.

- BLOCK is used if it is decided that the traffic should always be denied, or blocked.

Since setting up policies is important within GFI WebMonitor. For more details on how to do it:

- Web Filtering and Web Browsing Policies (WebFilter Edition) click here.
- Download Control Policies (WebSecurity Edition) click here.

6. Reporting with GFI WebMonitor

All Editions of GFI WebMonitor provide real-time and historical reporting. GFI WebMonitor provides a real-time dashboard where you can instantly see information about the current Internet usage. This includes, number of urls requested, total bandwidth consumed, bandwidth per hour, number of current active connections, number of downloads scanned, number of items quarantined, current number of connections blocked by policies, and bandwidth trending over time.

Administrators no longer need to waste time going through logs to review users Internet activity. They can also see the current connections being made in the network and can cancel them in real time.

While the GFI WebMonitor dashboard has real-time reporting, GFI has produced an easy to use reporting facility called GFI WebMonitor ReportPack. GFI WebMonitor Report Pack takes the information GFI WebMonitor collects and runs scheduled reports and sends them via email on a regular basis.

Note: GFI WebMonitor ReportPack is a separate installation and requires the GFI Report Center. The GFI Report Center can be found here, and the GFI WebMonitor ReportPack can be found here.

The types of reports which can be created through GFI WebMonitor ReportPack include:

- **Bandwidth Reports**: Contain reports used by administrators to observe bandwidth consumption.
- **Hits Reports**: Contains reports used to extract statistical data about website hits.
- **Threat Reports**: Contains reports used to extract statistical data about blocked websites.
- **Web Usage Trend Reports**: Contains reports used to extract the web usage trend of Users.

To see sample ReportPack reports go **here**.

Full documentation on GFI WebMonitor ReportPack can be found **here**.

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

33 North Garden Avenue, Suite 1200, Clearwater, FL 33755, USA
Telephone: +888 688-8457 (US/Canada)
Fax: +1 727 562-5199
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

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.