SmartGuide

This SmartGuide is an important tool to enhance your success with the GFI WebMonitor® product.

GFI WebMonitor™

Welcome to GFI WebMonitor. This solution gives you complete control, in real time, to monitor what users are browsing on the Internet, ensuring any files they download are free of viruses and other malware.

1 Introduction

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

- An overview of GFI WebMonitor
- Reasons why customers purchase GFI WebMonitor
- Major points to consider before deploying the product.

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.

Through this guide and a little planning, 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 access 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 at http://www.gfi.com/contact-us or at http://www.gfi.com/support/products/gfi-webmonitor.

2 Product overview

Let's start with an overview of what GFI WebMonitor can do. Simply stated, GFI WebMonitor enables you to monitor, manage and secure Internet activity. It provides visibility into:

- what web sites your users are browsing
- which applications they are using
- the types of files being downloaded
- how much time they are spending on the Internet
- the amount of bandwidth being consumed, and more.

GFI WebMonitor allows you to define Internet and Application filtering policies to help enforce an effective Internet Usage Policy. 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.

NOTE

An Internet Usage Policy is the business policies and practices that you would like to enforce on your network. At a basic level an Internet usage policy aims to:

- Increase employee productivity by controlling access to unproductive websites.
- Control downloads and reduce risks and threats associated with viruses/malware and other potential problems associated with the types of files employees download.
- Block malicious, vulnerable and phishing URLs

For more details on implementing an Internet Usage Policy, click here.

3 Why do customers purchase GFI WebMonitor?

Based on our experience, below are the top six (6) reasons GFI customers purchase GFI WebMonitor:

1. Reduce costs associated with bandwidth or avoid bandwidth hogs due to unauthorized internet activity.
2. To ensure line of business applications have sufficient bandwidth to deliver their functionality.
3. To optimize productivity by blocking, soft-blocking or limiting access to unproductive internet content such as games, social media, etc.
4. To protect employees and secure corporate network against Internet threats.
5. To meet legal and/or compliance requirements* by:
    - protecting your system resources
    - securing confidential data from malware/spyware or viruses
    - protecting users from doing illegal downloads or illicit website access.
6. To enforce the company's Internet Usage Policy.

ⓘ *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.

4 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 information in this SmartGuide, you have any questions or want to discuss any points, 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

4.1 Determining license count

A GFI WebMonitor unit is called 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:

Option	Description
Authenticated	A seat is defined as a user when there is an authenticated connection. GFI WebMonitor records the username of the user making the connection.
Not authenticated	A seat is defined as an IP address for unauthenticated connections. GFI WebMonitor records the IP address of the computer making the connection.

When the use count exceeds the licensed count (number of paid licenses), GFI WebMonitor will notify the Administrator to acquire additional licenses.

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

Connection	Number of licenses consumed
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 Users or IP addresses added to the License Exclusion List	0
Two (2) authenticated users making connection from the same machine	2

4.2 System installation requirements

4.2.1 Software

Type	Software requirements (x86 and x64)
Supported Operating Systems	Microsoft Windows Server 2003 Microsoft Windows Server 2008 Microsoft Windows Server 2008 (R2) Microsoft Windows Server 2012 (R2) Microsoft Windows 7 Microsoft Windows 8(8.1) Microsoft Windows 10
Gateway and Simple Proxy Modes - Other server side required components	Microsoft.NET® Framework 4.0/4.5/4.6 IIS® Express SQL Server® Express 2005 or later SQL Server® 2005 or later (for reporting purposes) Gateway Mode - Other required components
Gateway Mode - Other required components	Routing and Remote Access configuration on Windows® Server 2003/2008
GFI WebMonitor Agent	Windows® Vista SP2 or later
Supported Internet browsers	Server side (for the main product console): Microsoft Internet Explorer 10 or later Google Chrome (v36 or later) Mozilla Firefox (v31 or later) Client side: Internet Explorer 8 or later Google Chrome (v36 or later) Safari Mozilla Firefox v. 31 or later Note Any client browser is supported for the main product functions, including mobile browsers, and other versions of the supported browsers; however in order to display block / warn messages properly, one of the above browsers is required.

4.2.2 Hardware

Table 1: Minimum hardware requirements for 32 bit systems

x86 Architectures	Minimum hardware requirements
Processor	2.0 GHz processor
Memory	4 GB RAM
Physical storage	12 GB of available disk space.

Table 2: Minimum hardware requirements for 64 bit systems

x64 Architectures	Minimum hardware requirements
Processor	2.0 GHz processor (multi-core recommended)
Memory	8 GB RAM
Physical storage	12 GB of available disk space.

ⓘ NOTE
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. Hardware specs are also a factor of the amount of users and network traffic using GFI WebMonitor.

Other Hardware

Component	Hardware requirements
Network card	2.0 GHz processor (multi-core recommended)
Router	A Router\gateway that supports traffic forwarding or port blocking when installing in Simple Proxy Mode.

4.3 Choosing between Basic and Integrated authentication

GFI WebMonitor can be configured to enforce authentication using one of two methods:

Option	Description
Network card	Select if user is required to provide login credentials when new Internet sessions are launched
Router	This option enables GFI WebMonitor proxy to authenticate users by using the client machines access control service. User is not prompted to provide login credentials when new Internet sessions are launched. (Recommended)

For more information, click here.

4.4 Configuring client Web browsers

GFI WebMonitor requires that you configure client web browsers to make use of the GFI WebMonitor machine as the proxy server for web traffic requests. To do this you can:

- Manually configure client web browsers to point to the machine on which GFI WebMonitor is installed as the proxy server, or Use Group Policy to automatically configure all the web browsers you wish to monitor at one go,

or

- Enable WPAD in GFI WebMonitor to let client browsers detect the proxy settings automatically.

Refer to the GFI WebMonitor Administrator Guide for more information on each configuration option listed above.

ⓘ NOTE
Add the following Note: If you are running GFI WebMonitor in Transparent mode, this step is not required.

ⓘ NOTE
If you are going to apply policies to users/groups, you MUST set GFI WebMonitor to REQUIRE authenticated connections. If you don't set GFI WebMonitor to require authenticated connections, policies created for users/groups will not be applied. For more information, refer to Choosing between Basic and Integrated authentication (page 5).

4.5 Setting up usage policies

GFI WebMonitor makes use of flexible policies that help create and enforce a suitable Internet Usage Policy based on your company needs. These policies are sets of rules that define how your users are going to access the Internet through web browsers or applications (such as peer-to-peer or chat apps). Policies are easy to customize and configure. They can be applied to all your users or on a more granular level to specific IPs, users, or groups. Policies can be enforced during specific hours, or remain on continuously.

! IMPORTANT
GFI WebMonitor policies work in a hierarchical order. The policies at the top take precedence over the ones beneath. It is possible to change the order of the configured policies by dragging a policy to the desired place in the list, however this may have repercussions on your setup.

Policies allow you to control:

- Internet access to categories of websites.
- Browsing time and download bandwidth based on thresholds
- Access to web applications to cut down on elevated business costs, while solving productivity issues and optimizing bandwidth management .
- File downloads based on file types, while also safeguarding your network by scanning downloaded files for viruses, malware and phishing scams.

When creating a policy, you have to decide what action should be taken when any of the set criteria is met. The product provides for four (4) actions: Allow, Block, Monitor, Warn.

Action	Description
Allow	Used in cases where a policy has been created to ensure that specific traffic is always accessible. There is no further action by GFI WebMonitor.
Memory	Used if it is decided that the traffic should always be denied, or blocked. Subsequent policies are not applied.
Monitor	Used when you want to allows access to requested content but would like GFI WebMonitor to continue processing subsequent policies.
Warn	The user receives a notification that the requested content breaches a configured policy, but enables user to access the content. Subsequent policies are not applied.

Setting up policies is important within GFI WebMonitor. Refer to the GFI WebMonitor Administrator Guide for more information on how to configure and work with policies.

4.6 Working with reports

GFI WebMonitor provides real-time and historical reporting.
Use the Real-Time Traffic dashboard to instantly see information about current Internet usage.
Available data in this dashboard includes:

Number of URLs requested, total bandwidth consumed, bandwidth per hour, number of current active connections, number of downloads scanned, 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. Data collected by GFI WebMonitor is used by the internal reporting engine to leverage relevant information which is then presented in a variety of reports. These reports can be scheduled for automatic generation and sent via email on a regular basis. Available reports are classified under the following categories:

Category	Description
Bandwidth Reports	Reports used by administrators to observe bandwidth consumption.
Activity Reports	Reports used to extract statistical data about user Internet activity.
Security Reports	Reports used to extract statistical data about security issues and threats identified by GFI WebMonitor.

Existing reports can be modified as desired, and can be also cloned to create new custom reports.

5 How to easily configure GFI WebMonitor for first use

After performing the installation, use the Configuration Wizard to configure GFI WebMonitor for first use. The wizard guides you through a series of six (6) steps to ensure that your installation is successful. It takes only a couple of minutes to complete the wizard and then you can immediately start using GFI WebMonitor.

The GFI WebMonitor Configuration Wizard takes care of the following steps:

Option	Description
Configure connection settings	Choose your Network Mode depending on your current network setup. Establish a connection between your internal network and the Internet through the GFI WebMonitor server.
Enter your License key	Key in a valid license to use GFI WebMonitor. This can either be a trial license or a regular license key obtained on renewal.
Configure HTTPS Scanning	Configure HTTPS scanning to monitor and block encrypted traffic.
Set up the Database	Configure the database to use with GFI WebMonitor where collected data is stored. Use the embedded (Firebird) database only during the evaluation period. It is highly recommended to switch to a Microsoft SQL Server based database for live systems.
Define Admin Credentials	Key in the admin credentials required by the GFI WebMonitor services to control internal security engines, manage updates, send notifications and control data displayed in the User Interface. The GFI WebMonitor services are Windows services installed automatically during installation and require administrative privileges to operate.
Setup Email notification settings	Provide the email addresses required by GFI WebMonitor to send messages containing information related to tasks such as auto-updates and licensing issues.
Configuring Internet Browsers to use a Proxy Server	If you have not configured WPAD, ensure that proxy settings of client machines are configured to use GFI WebMonitor as the default proxy. This ensures that Internet traffic is routed through GFI WebMonitor.

ⓘ NOTE

The Configuration Wizard is launched automatically after installing GFI WebMonitor or manually from the **Settings** menu.

WEBMONN dec15

GFI®

www.gfi.com

For a full list of GFI offices/contact details worldwide,
please visit: www.gfi.com/contact-us

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.