



GFI WebMonitor

for ISA Server

Real-time HTTP/FTP monitoring, anti-virus & access control

Research by IDC shows that up to 40% of employee internet activity is non-work related. As a network administrator, you need tools to control employees' web browsing activities and to ensure that any files downloaded are free of viruses and other malware. GFI WebMonitor for ISA Server boosts employee productivity by giving you control over what users are browsing and downloading in real-time.

GFI WebMonitor comes with WebGrade, a 100% human-reviewed site categorization database that gives you control over what sites users can browse and block access to websites in particular categories, such as adult, online gaming, personal email, P2P, Facebook, Myspace, travel websites and more.

GFI WebMonitor allows you to monitor what files employees are downloading, to block file-types such as mp3s and to scan all files for viruses, spyware and malware using multiple anti-virus engines. GFI WebMonitor also lowers the risk of social engineering by blocking access to phishing websites through the use of an auto-updatable database of phishing URLs.

GFI WebMonitor for ISA Server is available in 3 editions:

- **UnifiedProtection Edition:** Combines both WebFilter and WebSecurity editions.
- **WebFilter Edition:** Includes URL filtering and website categorization.
- **WebSecurity Edition:** Includes anti-virus, anti-phishing and spyware detection.

All editions support Microsoft ISA Server 2004 and Microsoft ISA Server 2006.

Features of GFI WebMonitor - UnifiedProtection Edition (common features)

The features below are available with all editions.

■ Monitor or block a connection in real-time

Administrators can see what websites the users are currently browsing and what files are being downloaded. An active connection, browsing session or download can be easily blocked by simply clicking on the block connection icon. For example, you may decide to interrupt the download of a large file that a user is downloading.

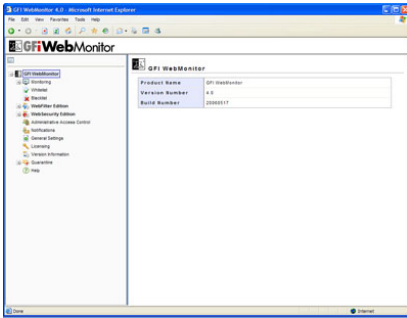
■ Monitor or block applications' hidden downloads

Some software applications automatically connect to their home pages to download updates using HTTP tunnelling. Although this can reduce administration, it can also present a security risk because unknown applications or trojans can use the same technique to download malicious files onto a user's PC, without the user knowing, including spyware, adware and pornware. GFI WebMonitor allows you to control which sites are allowed to distribute updates (for example www.microsoft.com).

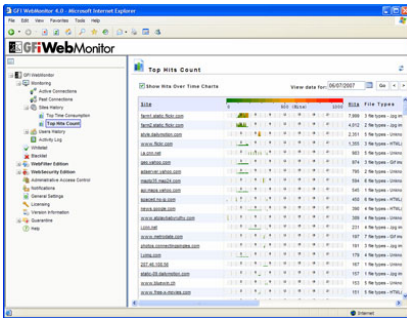
Benefits

Why use GFI WebMonitor?

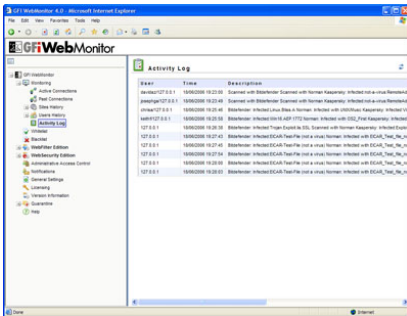
- Increase productivity by controlling your employees' web browsing habits
- Protect the network from dangerous downloads in real-time
- Reduce cyberslacking – time wasted by employees online
- Prevent data leakage through socially-engineered websites
- Benefit from multiple scanning engines to ensure that downloads are free of viruses and other malware.



GFI WebMonitor main screen

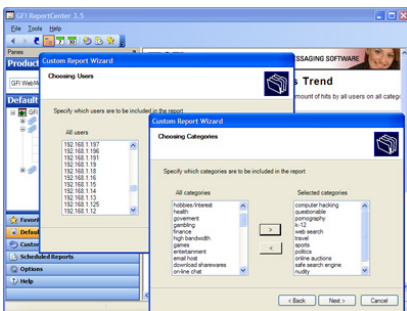


Monitors connections and provides statistics

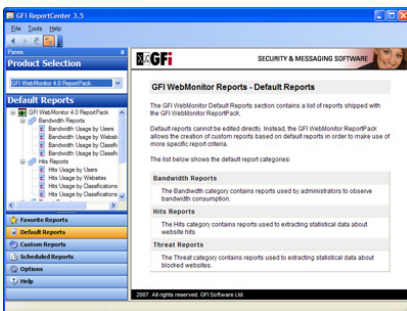


Monitors user online activity

GFI WebMonitor ReportPack



Custom report wizard



List of default reports

Monitor bandwidth

Through the user and site bandwidth monitoring features the administrator has the ability to track download and upload traffic and the number of URL hits over time, either on a user basis or on a website basis. Real-time monitoring may be achieved through drilldown reporting enhanced with graphs within the user interface.

Allow exceptions through whitelist and blacklists

Any URL/user/IP can be added permanently or temporarily to the whitelist or blacklist in order to bypass all web filtering and web security policies. For example, you may want to grant access to a particular user only to temporarily access his personal webmail account for a specified time period.

Controlled access to the configuration and monitoring interfaces

GFI WebMonitor allows you to select which users can access its configuration and monitoring interfaces. You can assign such rights based on either the IP of the computer from which access is being made or by the domain-authenticated username of the client trying to load the configuration. Only users in GFI WebMonitor's authorized users/IP list of will be given access.

Features of GFI WebMonitor - WebFilter Edition

WebGrade Database

GFI WebMonitor 4 comes with a human-reviewed site categorization database. This database allows administrators to set up filtering policies based on user/group/IP that provide control over what sites users can browse and block access to websites in particular categories, such as adult, online gaming, personal email, P2P, travel websites and social networking sites such as Facebook, MySpace and Bebo. Websites can either be blocked or else allowed through with an appropriate warning/notification.

Time-based filtering

Each of the web-filtering policies may be configured to work on a time schedule. This means that administrators can configure the product to allow users/groups to access certain websites during specific time windows; for example, employees can be allowed to access news and entertainment websites or access their webmail during break time.

Anti-phishing

GFI WebMonitor 4 protects the users from the potential risks of social engineering by blocking access to phishing websites through an auto-updatable database of phishing URLs.

Mitigate legal liability

Without the ability to exercise some form of control over what your users are browsing, you might be open to lawsuits. Employees can seek legal compensation if you do not shown due diligence in providing a work environment that is free of harassment. To provide this, you must install tools that allow you to block, or at least monitor, access to websites with inappropriate content such as pornography and other adult websites.

Features of GFI WebMonitor - WebSecurity Edition

■ Scan downloaded files with multiple anti-virus engines

GFI WebMonitor uses multiple virus scanners to scan files that are being downloaded. Using multiple scanners drastically reduces the average time to obtain virus signatures which combat the latest threats, and therefore greatly reduces the chances of an infection. The reason for this is that a single anti-virus company can never ALWAYS be the quickest to respond. For each outbreak, virus companies have varying response times to a virus, depending on where the virus was discovered, etc. By using multiple virus engines, you have a much better chance of having at least one of your virus engines up-to-date and able to protect against the latest virus. In addition, since each engine has its own heuristics and methods, one virus engine is likely to be better at detecting a particular virus and its variants, while another virus engine would be stronger at detecting a different virus. Overall, more virus engines means better protection.

■ Anti-virus protection through Norman Virus Control and BitDefender

GFI WebMonitor is bundled with Norman Virus Control and BitDefender. Norman Virus Control is an industrial strength virus engine that has received the 100% Virus Bulletin award 19 times running. It also has ICSA and Checkmark certification. BitDefender is a very fast and flexible virus engine that excels in the number of formats it can recognize and scan. BitDefender is ICSA certified and has won the 100% Virus Bulletin award and countless awards for its flawless protection. GFI WebMonitor automatically checks and updates the Norman Virus Control and BitDefender definition files as they become available. The GFI WebMonitor price includes updates for one year.

■ Malware (trojans, spyware, etc) blocking via Kaspersky – optional

To achieve even greater security and benefit from scanning via multiple virus engines, users can add the Kaspersky SuperSecure anti-virus engine, available as an optional add-on. The Kaspersky SuperSecure database includes support for the detection of malicious software that can perform remote administration, keyboard espionage, password detection, automatic dial-up to paid sites, automatic downloads of files containing explicit materials and more. GFI WebMonitor automatically checks and updates the Kaspersky definition files as they become available.

■ Protect against socially engineered phishing websites

Phishing is a social engineering technique that is maliciously used by hackers to acquire information such as usernames, passwords and credit card details by leading users to believe that they are passing on these details to the genuine company. Online shopping and credit card companies are amongst the most targeted phishing websites. GFI WebMonitor protects users from the potential risks of social engineering by blocking access to phishing websites. This is done through the use of an auto-updatable database of phishing URLs.

■ Control which file types users can download

You can create multiple user/group/IP based download control policies in order to block particular file types (such as Javascript, MP3, MPEG, exe, and more) from being downloaded by particular users. Dangerous files (such as trojan downloader programs) often attempt to penetrate a system masked as an innocuous files. GFI WebMonitor uses its built-in file signature scanner to analyze and detect the REAL filetype signatures of downloaded HTTP/FTP files.

System requirements

- Windows 2000 (SP4), 2003 operating system
- Microsoft ISA Server 2004 or later
- Internet Explorer 6 or later
- .NET Framework 2.0.

Awards



Download your evaluation version from <http://www.gfi.com/webmon/>

GFI Software
Magna House, 18 – 32 London Road
Staines, Middlesex
TW18 4BP
UK
Tel +44 (0) 870 770 5370
Fax +44 (0) 870 770 5377
sales@gfi.co.uk

GFI Software
15300 Weston Parkway
Suite 104
Cary, NC 27513
USA
Tel +1 (888) 243-4329
Fax +1 (919) 379-3402
sales@gfiusa.com

GFI Asia Pacific Pty Ltd
83 King William Road
Unley 5061
South Australia
Tel +61 8 8273 3000
Fax +61 8 8273 3099
sales@gfiap.com

GFI Software
GFI House
San Andrea Street
San Gwann SGN 1612
Malta
Tel +356 21 382418
Fax +356 21 382419
sales@gfi.com

Microsoft
GOLD CERTIFIED
Partner

GFI
www.gfi.com