GFI

- NETWORK SECURITY
- CONTENT SECURITY
- MESSAGING

GFI MailEssentials
for Exchange/SMTP/Lotus

GFI MailSecurity
for Exchange/SMTP/Lotus

GFI MailArchiver
for Exchange

GFI FAXmaker
for Exchange/SMTP/Lotus

GFI LANguard
Network Security Scanner

GFI EventsManager

GFI EndPointSecurity

GFI NETWORK ServerMonitor

GFI WebMonitor
for ISA Server

Overview of GFI products

GFI MailEssentials — Anti-spam, anti-phishing and email management

GFI MailEssentials for Exchange/SMTP/Lotus offers spam and phishing protection and email management at server level. GFI MailEssentials offers a fast set-up and a high spam detection rate using Bayesian analysis and other methods – no configuration required, very low false positives through its automatic whitelist, and the ability to automatically adapt to your email environment to constantly tune and improve spam detection. GFI MailEssentials also adds email management tools to your mail server: disclaimers, email archiving and monitoring, Internet mail reporting, list server, server-based auto replies and POP3 downloading.

GFI MailSecurity — Email anti-virus, content policies, exploit detection and anti-trojan

GFI MailSecurity for Exchange/SMTP/Lotus is an email content policies, exploit detection, threats analysis and anti-virus solution that removes all types of email-borne threats before they can affect your email users. GFI MailSecurity's key features include multiple virus engines, to guarantee higher detection rate and faster response to new viruses; email content and attachment checking, to quarantine dangerous attachments and content; an exploit shield, to protect against present and future viruses based on exploits (e.g., Nimda, Bugbear); an HTML Sanitizer, to disable HTML scripts; a Trojan & Executable Scanner, to detect malicious executables; and more.

GFI MailArchiver — Email archiving of internal and external email

GFI MailArchiver for Exchange provides easy-to-use corporate email archiving, enabling you to archive all internal and external email into one or multiple databases, heavily reducing reliance on PST files. This allows you to provide users with easy, centralized access to past emails via a web-based search interface and the ability to quickly restore emails through a OneClick Restore process. GFI MailArchiver also aids you to meet the requirements of your email retention policy and helps you to fulfill regulatory email storage requirements such as the Sarbanes-Oxley Act. GFI MailArchiver for Exchange leverages the journaling feature of Exchange Server 2000/2003 and therefore provides unparalleled scalability and reliability at a competitive cost.

GFI FAXmaker — Network fax server for Exchange/SMTP/Lotus

GFI FAXmaker for Exchange/SMTP/Lotus is the leading network fax server. It integrates with Exchange Server, Lotus Domino and popular SMTP servers, allowing users to send and receive faxes and SMS/text messages directly from their email client. By leveraging your email infrastructure and Active Directory, GFI FAXmaker achieves unparalleled scalability, reliability and hassle-free administration. GFI FAXmaker has won the Windows IT Pro Magazine (formerly Windows & .NET) Readers' Choice Award for 3 years running.

GFI LANguard — Network vulnerability scanning, patch management and auditing

GFI LANguard Network Security Scanner (N.S.S.) is an award-winning solution that allows you to scan, detect, assess and rectify any security vulnerabilities on your network. As an administrator, you often have to deal separately with problems related to vulnerability issues, patch management and network auditing, at times using multiple products. However, with GFI LANguard N.S.S., these three pillars of vulnerability management are addressed in one package. Using a single console with extensive reporting functionality, GFI LANguard N.S.S.'s integrated solution helps you address these issues faster and more effectively.

GFI EventsManager **Event monitoring, management and archiving**

GFI EventsManager is an event monitoring, event management and archiving solution that provides network-wide control and management of Windows event logs, W3C logs, Syslog events and SNMP Traps generated by network resources and hardware such as firewalls, routers and sensors. GFI EventsManager monitors an extended range of hardware products, reports on the health and operational status of each one and collects data for analysis.

GFI EndPointSecurity **Comprehensive control on use of iPods, USB drives and other portable devices**

GFI EndPointSecurity offers you network-wide control of data flow via portable storage devices, allowing you to prevent users from taking confidential data or introducing viruses and Trojans to your network. GFI EndPointSecurity allows you to actively manage user access to media players (including iPod and Creative Zen), USB sticks, CompactFlash, memory cards, PDAs, Blackberries, mobile phones, CDs, floppies and other endpoint devices.

GFI NETWORK ServerMonitor **Network server monitoring software**

GFI Network Server Monitor automatically monitors your network and servers for failures and allows administrators to fix and identify issues before users report them. Alerts can be sent by email, pager or SMS. Actions, such as rebooting a machine, restarting a service or running a script, can be done automatically.

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

GFI WebMonitor is a utility for Microsoft ISA Server that allows you to monitor the sites users are browsing and what files they are downloading – in real-time. In addition it can block access to adult sites as well as performing anti-virus scanning on all downloads. GFI WebMonitor is the perfect solution to transparently exercise a degree of access control over users' browsing habits and ensure legal compliance – in a manner that will not alienate your network users!

GFI MailEssentials

for Exchange/SMTP/Lotus

Anti-spam, anti-phishing and email management

Every day businesses receive thousands of fraudulent, inappropriate and offensive emails. Deleting spam is time consuming, email server performance is affected and the security of your network is at risk from malicious emails. With over 60 awards to its name, 80,000 satisfied customers and unbeatable price-performance, GFI MailEssentials for Exchange/SMTP/Lotus is a best-of-breed anti-spam package that is easy to set up, that captures over 98% of spam and that also eliminates the need to install and update anti-spam software on each desktop.

GFI MailEssentials uses various techniques such as Bayesian filtering to achieve such a high spam detection rate whilst its white-listing technology guarantees what is possibly the lowest level of false positives in the industry. This technology enables the software to automatically adapt to your email environment and constantly tune and improve spam detection.

GFI MailEssentials also detects and blocks phishing emails, and stops the latest in spam threats, such as attachment spam. GFI MailEssentials also adds email management tools to your mail server: disclaimers, mail monitoring, Internet mail reporting, list server, server-based auto replies and POP3 downloading.

Server-based anti-spam and anti-phishing

GFI MailEssentials is server-based and installs on the mail server or at the Gateway, eliminating the deployment and administration hassle of desktop-based anti-spam and anti-phishing products. Desktop-based software involves training your users to create anti-spam rule sets, and subsequently users have to spend time updating these rules. Besides, this system does not prevent your server message stores from filling up with spam.

Benefits

Why choose GFI MailEssentials for anti-spam?

- Support for the industry leading messaging platforms including Microsoft Exchange 2000, 2003, 2007 and Lotus Domino
- Highest spam detection rate (98%) because of its Bayesian filtering technology
- Lowest false positives through its patent pending auto whitelist feature
- Server-based install, no client software required
- Voted MSExchange.org Readers' Choice Award Winner in the Anti-Spam Category four times
- #1 server anti-spam solution at unbeatable pricing – over 80,000 installations!

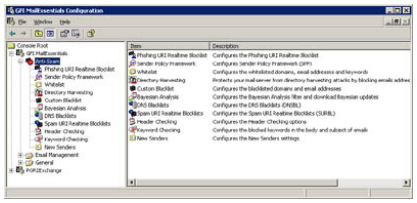
Bayesian filtering technology

Bayesian filtering is widely acknowledged by leading experts and publications as the best way to catch spam. A Bayesian filter uses a mathematical approach based on known spam and ham (valid email). This gives it a tremendous advantage over other spam solutions that just check for keywords or rely on downloading signatures of known spam. GFI's Bayesian filter uses an advanced mathematical formula and a dataset which is 'custom-created' for your installation: The spam data is continuously updated by GFI and is automatically downloaded by GFI MailEssentials, whereas the ham data is automatically collected from your own outbound mail. This means that the Bayesian filter is constantly learning new spam tricks, and spammers cannot circumvent the dataset used. This results in a 98+% spam detection rate, after the required two-week learning period. In short, Bayesian filtering has the following advantages:

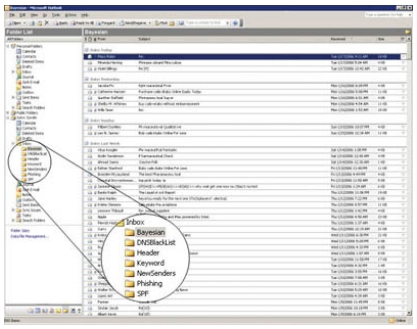
- Looks at the whole spam message, not just keywords or known spam signatures
- Learns from your outbound email (ham) and therefore greatly reduces false positives
- Adapts itself over time by learning about new spam and new valid email
- Dataset is unique to your company, making it impossible to bypass
- Multilingual and international.

Downloads updates to spam profile database

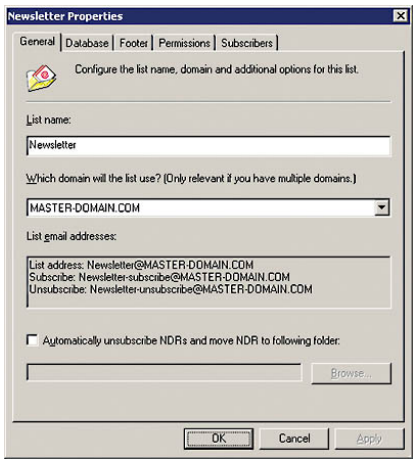
GFI MailEssentials can download updates to the Bayesian spam profile database from the GFI site, ensuring that it recognizes the latest spam and spamming techniques. GFI maintains the spam profile database by working with a number of spam collection organizations that continually supply spam samples.



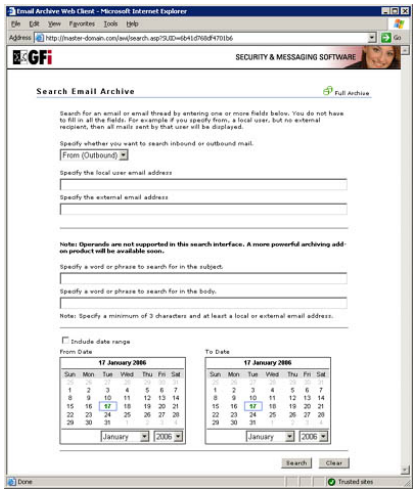
GFI MailEssentials configuration



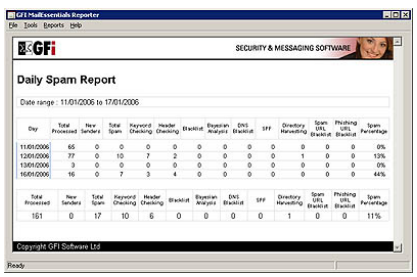
Users can review spam email



Newsletter list options



Search email archive from anywhere via the web-based interface



Create advanced reports on spam filtering

Protect your users against the menace of phishing emails

GFI MailEssentials' anti-phishing module detects and blocks threats posed by phishing emails by comparing the content of the scam with a constantly updated database of blacklisted mails, thereby ensuring all the latest phishing emails are captured. As extra protection, it also looks for typical phishing keywords in every email sent to your organization.

Sort spam to users' junk mail folders

GFI MailEssentials gives you the flexibility to choose what to do with spam. You can delete it, move it to a folder, forward the spam mail to a public email address or folder, or send it to individual customizable folders (for example, a "junk mail" folder) in the end-users' inboxes. This allows users to easily review mail that has been flagged as spam.

List server for newsletter lists and discussion lists

A list server is the best method for distributing company newsletters, since it automates the process of allowing users to subscribe and unsubscribe (required by anti-spam regulations). However, until now, list servers have been expensive and difficult to administer and they did not integrate with Exchange Server. GFI MailEssentials integrates with Exchange and can use Microsoft Access or Microsoft SQL Server as the backend. Both newsletter lists and discussion lists are supported.

Easy tuning of the Bayesian engine via public folders

Administrators can easily tune the Bayesian engine by dragging and dropping spam or ham to the appropriate public folder. GFI MailEssentials learns from the spam and ham that it picks up from these folders and further improves its spam detection rate. Administrators can control access to this feature through the use of Public Folder security.

Allow users to whitelist or blacklist via public folders

GFI MailEssentials allows users to whitelist or blacklist senders simply by dragging and dropping the appropriate mail to a public folder. This gives users more control and reduces administration. Administrators can control access to this feature through the use of Public Folder security.

Eliminate hard to catch image, PDF, Excel and ZIP spam

With spammers controlling tens of thousands of zombie machines, these large botnet armies have become one of the leading sources of spam. The Botnet/Zombie check in GFI MailEssentials eliminates hard to catch attachment spam such as image spam, PDF spam, Excel and ZIP spam. The attachment spam check filters this attachment spam quickly, efficiently and with a very low rate of false-positives.

Email header analysis and keyword checking

GFI MailEssentials intelligently analyzes the email header and identifies spam based on message field information. It detects forged headers, encoded IPs, spam mutation, spam sent from invalid domains, and more. It also enables you to configure keywords to check for spam using keyword checking.

Third party DNS blacklists (DNSBL) checking

GFI MailEssentials supports DNS blacklists (real time black hole lists), which are databases of known spammers. If the sending mail server is on one of those lists, it marks the email as spam. GFI MailEssentials supports popular third party blacklists such as ORDB, SpamHaus, Spamcop and also enables administrators to configure custom RBL servers.

Support for multiple third party SURBL servers

GFI MailEssentials checks email content against SURBL servers. Administrators can configure multiple SURBL servers, add their own and also define the priority of which server should be checked first. More information on SURBL can be found at http://www.surbl.org.

Automatic whitelist management reduces false positives

Whitelists enable you to ensure that email from particular senders or domains are never flagged as spam, permitting more stringent anti-spam rules. GFI MailEssentials includes a patent-pending automatic whitelist management tool, which automatically adds outgoing mail recipients to your whitelist. This greatly reduces false positives, without any need for additional administration. Whitelists can also be built based on domain names, email addresses and keywords.

Instant view of emails from new senders

The New Senders feature provides users with an instant view of emails sent from people they never had previous contact with, thereby helping users to better organize emails in their email client. If an email is not found to be spam by the GFI MailEssentials anti-spam modules and is also not on the whitelist, then the New Senders module has the ability to move the email to a user's subfolder, for example, Inbox\NewSenders.

Eliminates directory harvesting

Spammers often try to guess recipient addresses by generating multiple random email addresses at a domain; they then send their spam mail to all those addresses. GFI MailEssentials checks the validity of ALL the email addresses included in the mail sent, either via a query to Active Directory or through support for LDAP, and if they are not all valid, marks the mail as spam.

Reports on spam filtering and email usage

The database-driven reporting engine allows you to create advanced reports on your inbound and outbound email. You can report on the amount of spam filtered and on rules which caught most spam. You can also generate reports on user, domain and mail server usage.

Support for SPF – the Sender Policy Framework

As most of today's spammers spoof email addresses, it is important to be able to check whether an email is genuine or if it has been sent from a forged sending address. This can be done via the Sender Policy Framework (SPF), which allows users to test whether a particular email originates from its claimed source. GFI MailEssentials is one of the first commercial anti-spam solutions to support this framework. Its SPF module automatically checks whether the mail from a particular company was actually sent by its registered mail servers. For more on SPF, visit http://www.openspf.org.

Set priorities for each anti-spam module

You can configure which method of capturing spam is to be given priority, and create your own hierarchical list. For example, the administrator can select that the whitelisting anti-spam feature must be applied first to all incoming mail, then Bayesian scanning, and so on.

Company-wide disclaimer/footer/header text

GFI MailEssentials enables you to add disclaimers to the top or bottom of an email. Text and HTML formats are supported. You can include fields/variables to personalize the disclaimer. You can also create multiple disclaimers and associate them with a user, group or domain.

Seamless integration with Exchange Server, Lotus Domino and other SMTP servers

GFI MailEssentials integrates seamlessly with Microsoft Exchange 2000/2003/2007: It installs on the Exchange SMTP service and does not require gateway configuration. Via the SMTP protocol, it also works with Exchange 5.5, Lotus Domino and other popular SMTP/POP3 servers.

Content checking, anti-virus and anti-trojan

Get anti-virus, email content checking and anti-trojan protection for your mail server with the GFI MailEssentials & GFI MailSecurity Suite. GFI MailSecurity for Exchange/SMTP is an email content checking, exploit detection, threats analysis and anti-virus solution that removes all types of email-borne threats before they can affect your email users.

System requirements

- Windows 2000/2003 - Pro, Server or Advanced Server or Windows XP Professional
- IIS5 SMTP service installed and running as an SMTP relay to your mail server
- Microsoft Exchange server 2000, 2003, 2007, 4, 5 or 5.5, Lotus Domino, or an SMTP/POP3 mail server
- For the list server feature, Microsoft Message Queueing Services is required
- Microsoft .NET Framework 2.0.

Awards

Download your evaluation version from http://www.gfi.com/mes/

GFI MailSecurity

for Exchange/SMTP/Lotus

Email anti-virus, content policies, exploit detection and anti-trojan

The need to monitor email messages for dangerous, offensive or confidential content has never been more evident. The most deadly viruses, able to cripple your email server and corporate network in minutes, are being distributed worldwide via email in a matter of hours. Products that perform single vendor anti-virus scanning do not provide sufficient protection. Worse still, email has become the means for installing backdoors (trojans) and other harmful programs to help potential intruders break into your network. Products restricted to a single anti-virus engine will not protect against email exploits and attacks of this kind.

Your only defense is to install comprehensive granular user-based email content policy and anti-virus software to safeguard your mail server and network. GFI MailSecurity acts as an email firewall and provides mail security by protecting you from email viruses, exploits and threats, as well as email attacks targeted at your organization.

Virus checking with multiple anti-virus scanning engines

GFI MailSecurity uses multiple virus scanners to scan inbound email. 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.

Benefits

Why choose GFI MailSecurity to protect against email viruses and malware?

- Support for the industry leading messaging platforms including Microsoft Exchange 2000, 2003, 2007 and Lotus Domino
- Multiple virus engines guarantee higher detection rate and faster response
- Unique Trojan & Executable Scanner detects malicious executables without need for virus updates
- Email Exploit Engine and HTML Sanitizer disable email exploits & HTML scripts
- Unbeatable price: USD 346 (25), USD 1104 (100) and USD 7284 (1000) mailboxes.

Scan against trojans and executables

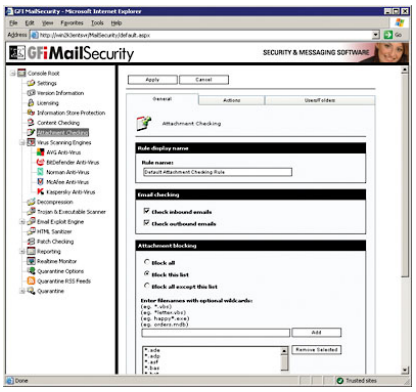
The GFI MailSecurity Trojan & Executable Scanner detects unknown malicious executables (for example, trojans) by analyzing what an executable does. Trojans are dangerous as they can enter a victim's computer undetected, granting an attacker unrestricted access to the data stored on that computer. Anti-virus software will NOT catch unknown trojans because it is signature-based. The Trojan & Executable Scanner takes a different approach by using built-in intelligence to rate an executable's risk level. It does this by disassembling the executable, detecting in real time what it might do, and comparing its actions to a database of malicious actions. The scanner then quarantines any executables that perform suspicious activities, such as accessing a modem, making network connections or accessing the address book.

Norman Virus Control & BitDefender virus engines are included

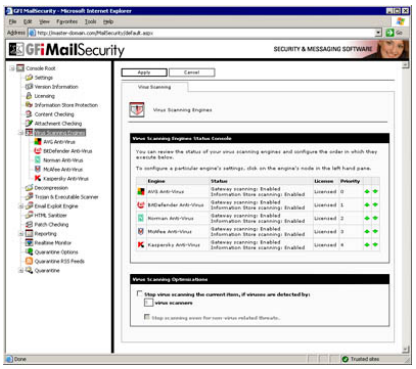
GFI MailSecurity is bundled with Norman Virus Control and BitDefender. Norman Virus Control is an industrial strength virus engine that has received the 100% Virus Bulletin award 32 times running. It also has ICSA and Checkmark certification. BitDefender is a very fast and flexible virus engine that excels in the number of formats it can recognize and scan. BitDefender is ICSA certified and has won the 100% Virus Bulletin award and the European Information Technologies Prize 2002. GFI MailSecurity automatically checks and updates the Norman Virus Control and BitDefender definition files as they become available. The GFI MailSecurity price includes updates for one year.

GFI MailSecurity

GFI MailSecurity configuration

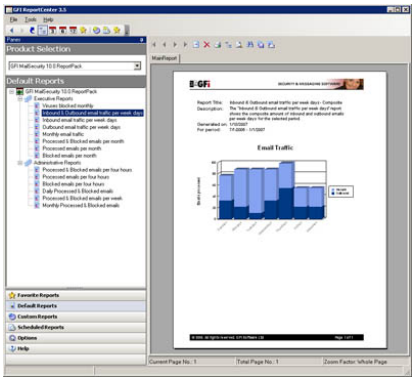


Configure attachment checking



GFI MailSecurity supports multiple virus engines

GFI MailSecurity ReportPack



User interface

Kaspersky, McAfee and AVG virus engines (optional)

To achieve even greater security, users can add the Kaspersky, McAfee and/or AVG anti-virus engines as a third, fourth or fifth anti-virus engine or as a replacement to one of the other engines. Kaspersky Anti-Virus is ICSA-certified and is well known for the unsurpassed depth of its object scanning, the high rate at which new virus signatures are released and its unique heuristic technology that effectively neutralizes unknown viruses. The McAfee virus engine is particularly strong at detecting non-virus attacks such as rogue ActiveX controls. With 15 years of experience in the anti-virus industry, GRISOFT employs some of world's leading experts in anti-virus software, specifically in the areas of virus analysis and detection.

Automatic removal of HTML scripts

The advent of HTML email has made it possible for hackers/virus writers to trigger commands by embedding them in HTML email. GFI MailSecurity checks for script code in the email message body and disables these commands before sending the "cleaned" HTML email to the recipient. GFI MailSecurity is the only product to protect you from potentially malicious HTML email using a GFI patented process, safeguarding you from HTML viruses and attacks launched via HTML email.

Email exploit detection engine

GFI's Email Exploit Engine builds on GFI's leading research on email exploits, and safeguards you from future email viruses and attacks that use known application or operating system exploits. For example, GFI MailSecurity would have protected you against the Nimda and Klez viruses when they first emerged without needing any updates, because these viruses use known exploits. GFI SecurityLabs regularly finds new email exploits, and these are automatically downloaded by GFI MailSecurity. GFI MailSecurity is the only email security product to detect email exploits.

Spyware detection

GFI MailSecurity's Trojan & Executable Scanner can recognize malicious files including spyware and adware. GFI MailSecurity can also detect spyware transmitted by email via the Kaspersky virus engine (optional) which incorporates a dedicated spyware and adware definition file that has an extensive database of known spyware, trojans and adware.

Attachment checking

GFI MailSecurity's attachment checking rules enable administrators to quarantine attachments based on user and file type. For example, all executable attachments can be quarantined for administrator review before they are distributed to the user. GFI MailSecurity can also scan for information leaks, for example, an employee emailing a database. You can also choose to delete attachments like .mp3 or .mpg files.

Multiply the value of GFI MailSecurity with powerful reporting

The GFI MailSecurity ReportPack is a full-fledged reporting companion to GFI MailSecurity. From trend reports for management (ROI) to daily drill-down reports for technical staff; the GFI MailSecurity ReportPack provides you with the easy-to-view information you need to fully understand your email security patterns. Full automation and custom scheduling allow you true install-and-forget functionality! The GFI MailSecurity ReportPack offers several default and customizable reports that can be prepared on an hourly, daily, weekly or monthly basis including:

- Viruses blocked
- Inbound email traffic
- Outbound email traffic
- Total inbound and outbound email traffic
- Processed emails
- Blocked emails
- And more!

Granular user-based email content policies/filtering

Using GFI MailSecurity's powerful content policies rules engine, you can configure rule sets based on user and keywords that allow you to quarantine potentially dangerous content for administrator approval. In this way, GFI MailSecurity can also scan for offensive content.

Custom quarantine filters

GFI MailSecurity enables you to configure a series of search folders (similar to MS Outlook Search Folders) within the 'Quarantine Store', permitting you to manage quarantined emails better and faster. For example, you can set up a folder for emails that were quarantined by virus checking and another for emails quarantined by attachment checking for a particular user, allowing you to prioritize which folders you check first: It may be more important to examine the attachment checking folder first as it is more likely to contain emails that need to be approved and forwarded to users.

Enable easy quarantine folder monitoring through RSS feeds

GFI MailSecurity takes advantage of the power of RSS (Really Simple Syndication) feeds to simplify your work as an administrator in keeping an eye on your email quarantine store. Through RSS feeds, you will be informed of all new quarantined objects, avoiding the need to log onto the quarantine store to check for new updates manually.

Web-based configuration – enables remote management from any location

The product's web-based configuration allows you to configure and monitor the product and manage quarantined emails remotely from any computer that is equipped with a browser. This means that you can monitor and manage GFI MailSecurity from anywhere in the world.

Approve/reject quarantined email using the moderator client, email client or web-based moderator

GFI MailSecurity provides several options for moderating quarantined email. The moderator client gives you a familiar Windows interface for approving/rejecting email. The web-based moderator allows you to approve/reject emails from anywhere on your network. Alternatively, GFI MailSecurity can also forward quarantined emails to an email address, enabling you to use a public folder to distribute the quarantined items to multiple administrators.

System requirements

- Windows 2000 Server/Advanced Server (Service Pack 1 or higher) or Windows 2003 Server/Advanced Server or Windows XP
- Microsoft Exchange server 2000 (SP1), 2003, 2007, 4, 5 or 5.5, Lotus Domino, or any SMTP/POP3 mail server
- When using Small Business Server, ensure you have installed SP 2 for Exchange Server 2000 and SP1 for Exchange Server 2003
- Microsoft .NET Framework 1.1/2.0
- MSMQ – Microsoft Messaging Queuing Service
- Internet Information Services (IIS) – SMTP service & World Wide Web service
- Microsoft Data Access Components (MDAC) 2.8.

Awards

Download your evaluation version from http://www.gfi.com/mailsecurity/

GFI MailArchiver

for Exchange

Email archiving of internal and external email

Companies' dependency on email to do business brings with it various problems. Storage, backups, problematic PST files, access to old emails and legal compliance are some issues that arise. To tackle these issues you need GFI MailArchiver an email archiving and email management solution with auditing functionality that is cost-effective, easy to install and requires very little administrative effort.

GFI MailArchiver – which ships at an unbeatable price and offers unparalleled performance – is used by thousands of administrators to avoid the pains of PST file management because it reduces the company's dependency on these files. All email is stored in a central location that is easily accessible using a web browser and the PST migration tool ensures access to old emails stored in PST files on users' machines. Using the auditing functionality, management can access any email that is requested for ediscovery/compliance purposes and guarantee that these emails have not been tampered with.

With GFI MailArchiver, network administrators can:

- Manage and reduce mailbox quotas on Microsoft Exchange server
- Reduce reliance on cumbersome PST files
- Archive past, present and future emails into one or multiple databases and avoid complex backup plans to copy PST files from each employee's workstation.

With GFI MailArchiver, employees can:

- Access all email from anywhere in the world using their web browser
- Retrieve old and deleted emails on demand – with full thread and conversation
- Use advanced email search and 'Saved Search' capabilities.

With GFI MailArchiver, management benefits from:

- Access to emails if required for discovery and compliance purposes, internal inquiries and employee monitoring
- A safeguard in customer lawsuits
- Auditing functionality that guarantees stored emails are genuine and have not been tampered with
- A complete and secure archive of all company email.

Benefits

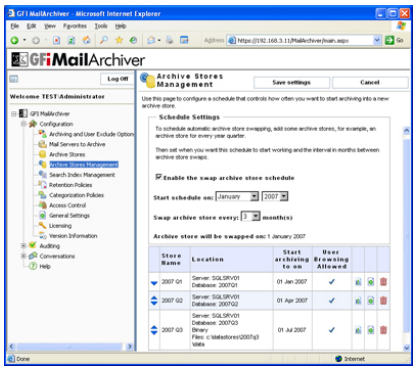
Why choose GFI MailArchiver?

- Cost-effective email archiving and management solution
- Tens of thousands of customers
- Support for the industry leading messaging platforms including Microsoft Exchange 2000, 2003 and 2007
- Reduce reliance on cumbersome PST files
- Employees can search for and retrieve old emails
- Auditing functionality to meet compliance/legal requirements.

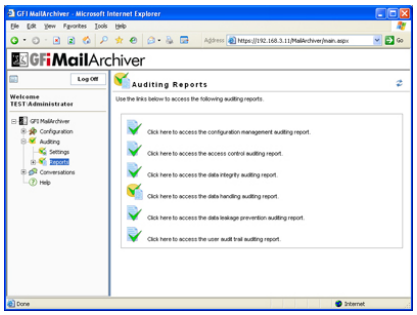
Features for the administrator

Integration with Exchange and other email servers

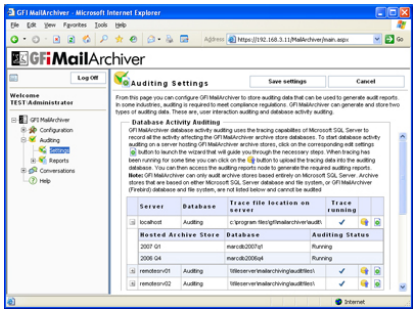
GFI MailArchiver leverages the journaling feature of Exchange Server, providing unparalleled scalability and reliability. Other email archiving solutions actually replace the email with a link to their database – this can be a point of failure and can bring down your entire email system. GFI MailArchiver works in parallel and does not touch the way Exchange works. GFI MailArchiver can be used with Exchange as well as other email servers with the capability of polling emails from a mail server which supports IMAP and Active Directory.



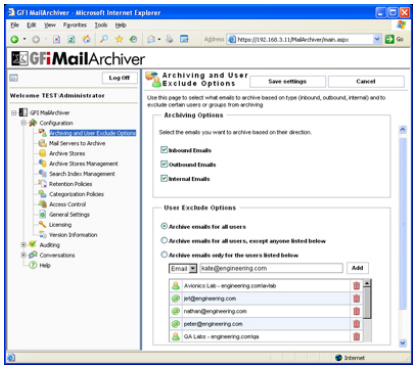
Archive stores management



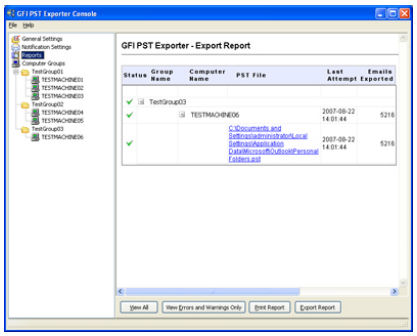
Auditing reports



Auditing database activity – auditing settings



Archiving and user exclude options



PSTExporter report

Automatically archive corporate email into one storage area

Your mail server is not the ideal place to store all organizational email: Over time this will cause a severe decline in email performance. Moving old emails into a database will keep your mail server performance high and email stores compact. You may archive your email in:

- **A SQL database:** Because email is stored in a standard SQL database, it is easy to backup and restore; no special Exchange backup tools are required. This setup is strongly recommended for high email volume environments.
- **Directly to an NTFS hard drive:** You may store email in a database that is located on an NTFS-formatted hard drive, saving you the license costs of Microsoft SQL Server! This setup is suitable for low email volume environments and for small enterprises intending to save on license costs of Microsoft SQL Server.

Multiple database support and 'automatic' database management support

It is possible to archive emails in multiple databases – this overrides the problem of having one large database that becomes slow and requires more maintenance. GFI MailArchiver allows you to automatically archive emails to a new database after a specified time, for example, every month or quarter.

Reduce email storage requirements

GFI MailArchiver compresses and decompresses attachments on the fly, which results in considerable savings in terms of storage when compared to storing attachments in the Exchange stores. In addition, storing email in a database is more space efficient than storing in PST files. An added advantage is that GFI MailArchiver archives only one copy of attachments sent to multiple recipients.

End PST hell

Using GFI MailArchiver for Exchange eliminates the need for users to archive their mail in PST files on local hard disks. These PST files end up being very large and are difficult to backup and search. Many users do not know how to organize their PST files properly. With GFI MailArchiver, users can browse to the web search interface and retrieve past email from the database, rather than having to dig through a store of PST files on disk to find a particular email.

Migrate old PST files stored on client machines

Through GFI MailArchiver's agent-based PST Exporter, you can archive emails processed by Microsoft Exchange prior to the installation of GFI MailArchiver. The GFI PST Exporter uses the GFI MailArchiver Import Service to transfer emails to an archive store without any end-user intervention. Agents save extracted emails in a destination folder and the GFI MailArchiver Import Service then imports the extracted emails into a GFI MailArchiver archive store.

Set up email retention and categorization policies

Setting up an email retention policy is critical and while email archiving is essential, retaining emails for an indefinite time is costly! With GFI MailArchiver you can create rules to delete one or more emails after a specific time, for example, you can delete all emails sent by the Marketing Department that are older than 7 years. In addition, GFI MailArchiver can help you to categorize emails by adding a label to the emails that meet a particular condition. For example, emails sent from the CEO, could be automatically labelled with [CEO].

Helps comply with Sarbanes-Oxley Act

By archiving all company email, GFI MailArchiver helps organizations to meet regulatory compliance such as the Sarbanes-Oxley Act. Under the Sarbanes-Oxley Act 2002 and Security and Exchange Commission (SEC) rules, public companies must prove that their internal controls and audit trails are sound and that their processes are capable of producing certifiably correct data. Companies must retain all correspondence created, sent, or received "in connection with an audit or review" of a public company for a period of seven years, during which time these records must be non-erasable and non-rewritable. This includes any "electronic records" such as email, particularly relating to subjects, departments or individuals involved in auditing procedures. Failure to comply is a crime, punishable by up to 10 years in jail.

Helps to comply to other acts and regulations

GFI MailArchiver is also a valuable tool that aids compliance with the following: E-Comm Act 2000, BS7799-2:2002, Enterprise Act 2002, Decreto del Presidente del Consiglio dei Ministri (8 febbraio 1999) and more.

Give viewing rights and exempt users from archiving email

GFI MailArchiver allows you to grant a user viewing rights to all email relating to a specific Active Directory Group, for example, the Sales Manager would be able to view all emails sent or received by his team. Also, if required, you can instruct GFI MailArchiver for Exchange not to archive email to/from particular users, for instance it is possible not to archive emails sent to/from the HR Manager.

Collect and archive emails in one geographical location

GFI MailArchiver provides the possibility of centralizing email archiving to one physical location by polling emails from multiple locations. For example, an organization that operates in the US, UK and Australia may want to archive email of all offices centrally in one location – the US office.

Audit your archived email to ensure they have not been tampered

GFI MailArchiver ships with auditing functionality that ensures all archived emails have not been tampered with. This is particularly important in industries and countries where regulations require organizations to monitor user activity and keep audit trails of such activity. GFI MailArchiver offers two types of auditing:

- Database activity auditing: Uses the tracing capabilities of Microsoft SQL Server to record all activity affecting the GFI MailArchiver archive databases.
- User interaction auditing: Record all users' activity whilst they are using the GFI MailArchiver web interface to browse email archive stores.

Features for the user

Access emails from any location through a browser

GFI MailArchiver allows users to access their emails from anywhere in the world by using a browser. Emails that had been deleted may also be seen (and restored).

Advanced email search and 'Saved Search' capabilities

Having a central store of email enables users to easily search through their past email and attachments (Microsoft Word, Excel, PDF, ZIP and many other formats). Once a search has been defined, the user has the possibility to save the search criteria for easy reference at a later date, similar to Microsoft Outlook Search Folders. For example, you may save a search that displays all email correspondence with client X.

OneClick Restore a single email to a mailbox

By simply clicking on a button, the user or the administrator can restore an email to a user's inbox in its original format. GFI MailArchiver restores any archived email (even deleted email) and these are resent to the user as an attachment.

Support for multilingual user interfaces

GFI MailArchiver provides support for multilingual user interfaces including English, Dutch, French, German, Italian, Russian, Spanish, Czech, Arabic, Japanese, Simplified Chinese and Traditional Chinese.

Other features:

- Printer-friendly support for printing emails

You're in good company...

Many leading companies have chosen GFI MailArchiver. Here are just a few: American International Movers, Inc, Autoflug GmbH (Germany), eCourier (UK) and many more.

System requirements

- Windows 2000 (Service Pack 3 or higher) or Windows 2003
- Access to Microsoft Exchange Server 2000 or later
- Microsoft .NET Framework 2.0
- Internet Information Services (IIS) – World Wide Web service.

Awards

Download your evaluation version from http://www.gfi.com/mailarchiver/

GFI FAXmaker

for Exchange/SMTP/Lotus

Network fax server for Exchange/SMTP/Lotus

GFI FAXmaker is a fax server that makes sending and receiving faxes an efficient, simple and cheaper process. The problems with manual faxing – waiting for the fax to go through, the need for printouts, physically walking to the fax machine – are solved because GFI FAXmaker allows users to receive and send faxes directly from their email client.

The benefits are numerous: Less time is spent sending, collecting and distributing faxes, noticeable cost savings and each fax received or sent is saved in digital format as an email. With tens of thousands of customers and numerous awards, GFI FAXmaker is the leading fax server on the market, offering reliability and enterprise functionality at an unbeatable price.

GFI FAXmaker is easy to install, requires little maintenance and integrates with existing messaging clients and customized solutions.

GFI FAXmaker integrates with your mail server, allowing users to send and receive faxes and SMS/text messages using their email client. The company can also search for and backup all faxes in the same way that emails are stored and retrieved on the network.

Active Directory integration reduces administration

GFI FAXmaker for Exchange/SMTP/Lotus was designed from the ground up to minimize its administration. It integrates with Active Directory and therefore does not require the administration of a separate fax user database. User-related settings can be applied to Windows users or groups directly.

Benefits

Why choose GFI FAXmaker for Exchange/SMTP/Lotus as your fax server?

- More than 10 years as the leading fax server on the market
- Award-winning solution; voted #1 by Windows IT Pro readers 3 years running
- Excellent price-performance ratio and immediate return on investment (ROI)
- Support Microsoft Exchange 2000, 2003, 2007, Lotus Domino and MDaemon
- Easy-to-use and learn
- Install and forget: No burden on administrators

Supports Microsoft Exchange, Lotus Domino and other SMTP servers

GFI FAXmaker integrates with Exchange Server 2000/2003/2007 via a standard Exchange SMTP connector. **There are no schema updates to Active Directory**. This makes GFI FAXmaker scalable and indifferent to new Exchange service packs and versions. Microsoft Exchange 5.5 is supported by creating a routing rule on the Exchange 5.5 SMTP connector. GFI FAXmaker can be installed on the Exchange server or on a separate machine, in which case no software has to be installed on the Exchange server itself! GFI FAXmaker also integrates with Lotus Domino and other popular SMTP servers.

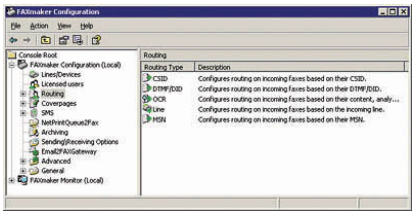
Fax over IP (FOIP) support

With the optional Brooktrout SR140 host-based module, GFI FAXmaker integrates with your existing IP PBX to offer Fax over IP (FOIP) capabilities without any hardware requirements. With FOIP you can easily send faxes over the Internet whilst integrating with the existing IP infrastructure. GFI FAXmaker's FOIP may also be used to implement Least Cost Routing (LCR); this results in cost-effectiveness that is achieved through a reduction in international calls dialed since calls are translated into a local call at the recipient's country. FOIP may only be employed if the appropriate FOIP-enabled software or devices are installed.

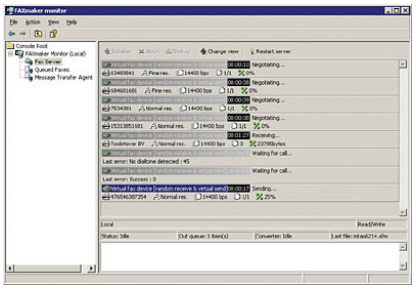
Supports Lotus Notes & SMTP/POP3 servers

GFI FAXmaker integrates via the SMTP/POP3 protocol with Lotus Notes and any SMTP/POP3 server. It can be installed on the mail server itself or on a separate machine. In the case of Lotus Notes, @FAX addressing is supported.

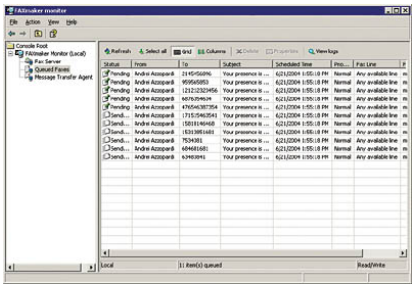
GFI FAXmaker



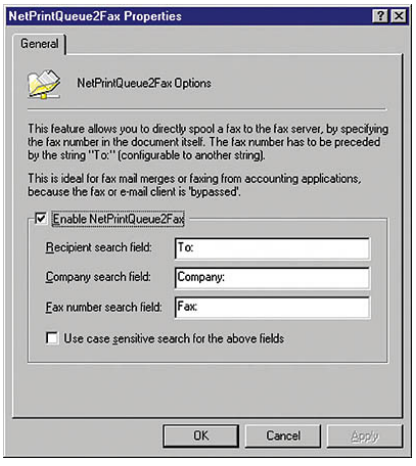
GFI FAXmaker configuration



The GFI FAXmaker server monitor

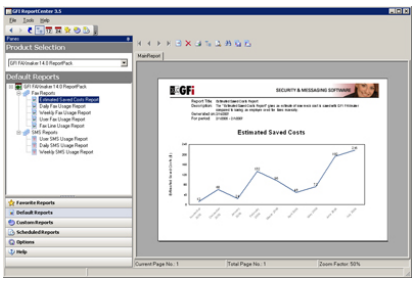


Monitor fax queue



Easy application integration using NetPrintQueue2FAX

GFI FAXmaker ReportPack



Estimated saved costs report

Automated fax delivery/inbound fax routing

GFI FAXmaker can automatically route incoming faxes to the user's mailbox or to a particular printer based on a DID/DDI/DTMF number or the line on which the fax was received. Faxes can also be forwarded to a public folder or assigned to a network printer per installed fax port.

SMS/texting gateway allows users to send SMS/text messages from their desktop

GFI FAXmaker's SMS gateway enables network users to send SMS messages from their desktop; this allows them to easily contact business colleagues and associates who are on the road or away from their desk. Using the SMS gateway rather than a mobile phone is faster (no need to use the phone pad) and saves users the cost of the SMS message. SMS messages can either be sent via an Internet-based SMS service or through a mobile phone or PCMCIA mobile card. The SMS gateway can also be used for administrative alerts, for example, to notify an administrator of critical system outages or application problems. Any email-enabled application can send SMS messages via the GFI FAXmaker SMS gateway. A central log of SMS messages permits the control of SMS use.

Multiply the value of GFI FAXmaker with powerful reporting

The integrated GFI FAXmaker ReportPack offers several default and customizable fax and SMS reports including:

- Fax usage per user or over a period of time
- Fax line usage
- SMS usage per user or over a period of time
- Estimated cost savings.

Supports multiple mail servers & clustering

Because of its flexible infrastructure, GFI FAXmaker can send and receive faxes for users on different mail servers. It can also support a mix of Exchange 5.5, Exchange 2000/2003 servers or even SMTP/POP3 servers. Active and passive clustering is fully supported because GFI FAXmaker does not require any software to be installed on the mail server itself; simply configure both mail servers in the cluster to be able to send and receive faxes via GFI FAXmaker.

Robust & scalable multi-line fax server

GFI FAXmaker includes a robust fax server, which can scale up to 32 lines per fax server using fax boards or active ISDN cards. For smaller installations, Fax modems can be used as well. GFI FAXmaker also supports the use of the Windows 2000/XP/2003 fax drivers for wider hardware support.

Native ISDN support

GFI FAXmaker natively supports ISDN, allowing you to use inexpensive active ISDN cards and get multi-line faxing and inbound routing at a fraction of the price of using multi-line fax boards.

Archive faxes to GFI MailArchiver, to SQL, or other archiving solution

GFI FAXmaker allows you to archive all faxes to GFI MailArchiver, a SQL database or to an email address. GFI MailArchiver is an email archiving solution that stores all mails in a SQL database and allows users to easily search for past emails and faxes. GFI FAXmaker can be configured to forward all faxes to GFI MailArchiver, allowing users to search for past faxes in the same way as emails. With the OCR module, faxes can also be searched based on what text they contained.

Optional OCR reading & routing module

The optional OCR module can be used to convert all incoming faxes to a readable text format using Optical Character Recognition (OCR) technology and then route the fax to the correct user by finding keywords related to a recipient, for example his first name, last name or job function. If GFI FAXmaker cannot match a recipient, it will route the fax to the default recipient/router. This feature is also especially handy if you plan to archive all faxes, since it makes searching for a particular fax much easier.

Junk fax filter

GFI FAXmaker includes a 'junk fax filter' that can auto-delete spam faxes on the basis of sender number.

Send faxes from any application

To send a fax, users print from their word processor to the GFI FAXmaker printer, or create a new message in their email client (e.g., Outlook or Outlook Web Access). The user then selects the recipient(s) of the fax from the Outlook Contacts list (address book) or enters the fax number directly. After clicking on the "Send" button, the fax is sent and the user receives a transmission report in his/her inbox.

Receive faxes in your email client – in fax or PDF format

GFI FAXmaker delivers faxes to the user's inbox in TIF – fax – format or Adobe PDF format. This enables users to check faxes from anywhere in the world, using either a normal desktop email client (for example, Outlook) or a web-based email client (for example, Outlook Web Access). Receiving faxes in PDF format means the fax can be forwarded to anybody, and it also allows for easy integration with document archiving systems or workflow software/procedures.

Allows you to send/receive faxes via your handheld or mobile

Via GFI FAXmaker's Email2Fax Gateway, the email clients of handhelds like the Blackberry and Pocket PC (2003 upwards) can be used to send faxes. The Blackberry and Pocket PC email clients can also receive faxes and fax reports as emails. The Blackberry devices have built-in PDF viewer that seamlessly integrate with GFI FAXmaker's PDF capabilities; most Pocket PC 2003 also ship with built-in PDF viewers. As long as they have image-viewing capabilities to view received faxes, GPRS mobile (cell) phones that are email-compliant can use GFI FAXmaker in the same way as handhelds.

Supports Outlook Contacts

There is no need to keep a separate fax address book - just select the recipient's "Business Fax" entry from the Outlook Contacts list or the Global Address Book: No need to duplicate address entries.

Attach Office documents, PDF, HTML and other files

Users can attach Microsoft Office, PDF, HTML and other files to their fax. These are rendered to fax format on the fax server. The 'Send to Mail Recipient' command, available in Microsoft Office and other applications, can therefore also be used to quickly send a document as a fax.

Automatic application integration & mail merges with NetPrintQueue2FAX

GFI FAXmaker's NetPrintQueue2FAX feature allows you to embed a fax number in a document and 'print to fax' from almost any application, from anywhere in the network - without having to enter the fax number separately. This feature is especially handy for accounting applications; an invoice can be faxed simply by embedding the fax number in the document. No application integration or development is required.

Fax broadcasting using Microsoft Office mail merge

Using the mail merge facility of Microsoft Word/Office, you can send personalized fax broadcasts. Because Microsoft Office supports ODBC, the recipient list can be retrieved from any data source, including Microsoft SQL Server, Microsoft Access and many more.

System requirements

- Windows 2000/2003/XP server machine with at least 256 MB of RAM and an 800 MHz processor
- A professional fax device: For a complete list go to http://kbase.gfi.com/showarticle.asp?id=KBID001220
- If you are installing GFI FAXmaker on a separate machine, the IIS SMTP service will need to be installed
- If using Windows 2000, ensure you have Service Pack 3 or later installed
- For more detailed system requirements please see the manual.

Awards

Download your evaluation version from http://www.gfi.com/faxmaker/

GFI LANguard

Network Security Scanner

Network vulnerability scanning, patch management and auditing

GFI LANguard Network Security Scanner (N.S.S.) is an award-winning solution that allows you to scan, detect, assess and rectify any security vulnerabilities on your network. As an administrator, you often have to deal separately with problems related to vulnerability issues, patch management and network auditing, at times using multiple products. However, with GFI LANguard N.S.S., these three pillars of vulnerability management are addressed in one package. Using a single console with extensive reporting functionality, GFI LANguard N.S.S.'s integrated solution helps you address these issues faster and more effectively.

GFI LANguard N.S.S. makes use of state of the art vulnerability check databases based on OVAL and SANS Top 20, providing over 15,000 vulnerability assessments when your network is scanned. GFI LANguard N.S.S. gives you the information and tools you need to perform multi-platform scans across all environments, to analyze your network's security health and effectively install and manage patches on all machines across different operating systems and in different languages. This results in a consistently configured environment that is secure against all vulnerabilities.

Voted the best commercial network security scanner by users of Nmap for two years running, named the winner in the Patch Management category in TechTarget's 2006 'Products of the Year' awards, and voted the winner in the security category of the Best of TechEd Awards 2007, GFI LANguard N.S.S. is the most complete vulnerability management solution in one convenient integrated package. GFI LANguard N.S.S. is an essential, cost-effective solution for businesses to safeguard their systems and networks from hacker attacks and security breaches.

Benefits

Why use GFI LANguard N.S.S.?

- Over 15,000 vulnerability assessments carried out across your network
- Reduces the total cost of ownership by centralizing vulnerability scanning, patch management and network auditing
- Provides customizable reports of scans performed across the whole network including applications and resources
- Helps IT administrators secure their networks faster and more effectively
- Prevents downtime and business losses due to vulnerability exposure
- #1 Windows commercial security scanner (voted by Nmap users for two years running) and Best of TechEd 2007 (security).

Integrated vulnerability management solution

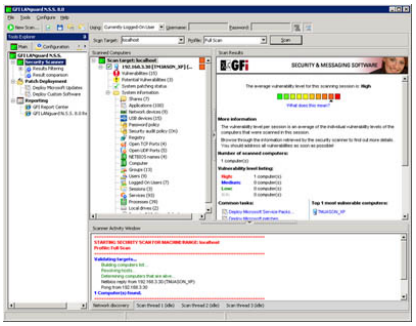
GFI LANguard Network Security Scanner (N.S.S.) is an award-winning solution that addresses the three pillars of vulnerability management: security scanning, patch management and network auditing through a single, integrated console. By scanning the entire network, it identifies all possible security issues and using its extensive reporting functionality provides you with the tools you need to detect, assess, report and rectify any threats.

- Vulnerability scanning
- Patch management
- Network and software auditing.

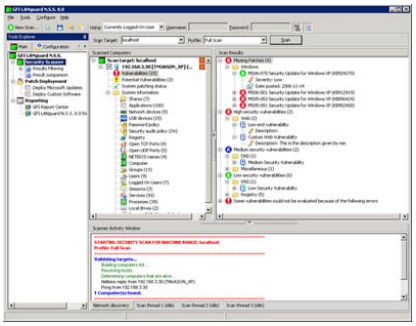
Vulnerability scanning

During security audits, over 15,000 vulnerability assessments are made and networks are scanned IP by IP. GFI LANguard N.S.S. gives you the capability to perform multi-platform scans (Windows, Mac OS, Linux) across all environments and to analyze your network's security health from a single source of data. This ensures that you are able to identify and rectify any threats before hackers manage to do so.

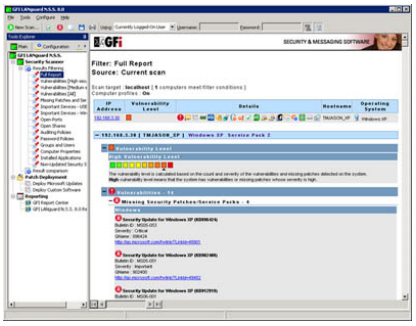
GFI LANguard Network Security Scanner



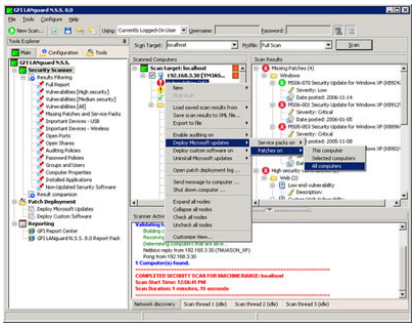
GFI LANguard Network Security Scanner main screen



Indicates vulnerabilities found

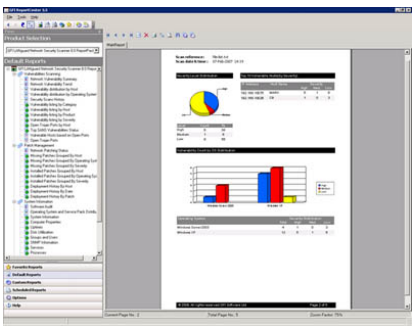


Extensive HTML security reports



Easily deploy patches network-wide

GFI LANguard Network Security Scanner ReportPack



Executive report showing network vulnerability summary

Identify security vulnerabilities and take remedial action

GFI LANguard N.S.S. scans computers, identifies and categorizes security vulnerabilities, recommends a course of action and provides tools that enable you to solve these issues. GFI LANguard N.S.S. also makes use of a graphical threat level indicator that provides an intuitive, weighted assessment of the vulnerability status of a scanned computer or group of computers. Wherever possible a web link or more information on a particular security issue is provided, such as a BugTraq ID or a Microsoft Knowledge Base article ID.

Extensive, industrial-strength vulnerabilities database

GFI LANguard N.S.S. ships with a complete and thorough vulnerability assessment database, which includes standards such as OVAL (2,000+ checks) and SANS Top 20. This database is regularly updated with information from BugTraq, SANS Corporation, OVAL, CVE and others. Through its auto-update system, GFI LANguard N.S.S. is always kept updated with information about newly released Microsoft security updates as well as new vulnerability checks issued by GFI and other community-based information repositories such as the OVAL database.

Ensures that third party security applications such as anti-virus and anti-spyware offer optimum protection

GFI LANguard N.S.S. also checks that supported security applications such as anti-virus and anti-spyware software are updated with the latest definition files and are functioning correctly. For example, you can ensure that supported security applications have all key features (such as real-time scanning) enabled.

Easily creates different types of scans and vulnerability tests

You can easily configure scans for different types of information; such as open shares on workstations, security audit/password policies and machines missing a particular patch or service pack. You can scan for different types of vulnerabilities to identify potential security issues. These include:

- **Open ports:** GFI LANguard N.S.S. scans for unnecessary open ports and checks that no port hijacking is in force.
- **Unused local users and groups:** Remove or disable User accounts no longer in use.
- **Blacklisted applications:** Identify unauthorized or dangerous software and add to blacklists of applications you want to associate with a high security vulnerability alert.
- **Dangerous USB devices, wireless nodes and links:** Scans all devices connected to USB or wireless links and alerts you of any suspicious activity.
- And much more!

Setup your own custom vulnerability checks

GFI LANguard N.S.S. allows you to easily create custom vulnerability checks through wizard-assisted custom-vulnerability condition setup screens. You can also write complex vulnerability checks using the GFI LANguard N.S.S. VBScript-compatible script engine. GFI LANguard N.S.S. includes a script editor and debugger to help with script development.

Easily analyze and filter scan results

GFI LANguard N.S.S. enables you to easily analyze and filter scan results by clicking on one of the default filter nodes. This enables you to identify, for example, machines with high security vulnerabilities or machines that are missing a particular service pack. Custom filters can also very easily be created from scratch or customized. You can also export scan results data to XML.

Patch management

When a scan is complete, GFI LANguard N.S.S. gives you all the functionality and tools you need to effectively install and manage patches on all machines across different Microsoft operating systems and products in 38 languages. Click here to view a full list. GFI LANguard also allows auto-downloads of missing patches as well as patch roll-back. Custom software can also be deployed. This results in a consistently configured environment that is secure against all vulnerabilities.

Automatically deploy network-wide patch and service pack management

With GFI LANguard N.S.S. you can easily deploy missing service packs and patches network-wide. GFI LANguard N.S.S. is the ideal tool to monitor that Microsoft WSUS is doing its job properly and it performs tasks WSUS does not such as deploying Microsoft Office and custom software patches. GFI LANguard N.S.S. also provides you with new features such as patch auto-download and patch rollback. It is also Unicode compliant and able to support patch management in all the 38 languages currently supported by Microsoft.

Deploys custom/third party software and patches network-wide

Besides deploying patches and service packs, GFI LANguard N.S.S. enables you to easily deploy third party software or patches network-wide. You can use this feature to deploy client software, update custom or non-Microsoft software, virus updates and more. The custom software deployment feature means you can do without Microsoft SMS, which is too complex and expensive for small to medium sized networks.

Network and software auditing

GFI LANguard N.S.S.'s auditing function tells you all you need know about your network – what USB devices are connected, what software is installed, any open shares, open ports and weak passwords in use. The solution's in-depth reports gives you an important and real-time snapshot of your network's status. Scan results can be easily analyzed using filters and reports, enabling you to proactively secure the network by closing ports, deleting users or groups no longer in use or disabling wireless access points.

Automatically receive alerts of new security holes

GFI LANguard N.S.S. can perform scheduled scans (for instance daily or weekly) and can automatically compare results to previous scans. Any new security holes or security setup changes discovered on your network are emailed to you for analysis. This enables you to quickly identify newly-created shares, installed services, installed applications, added users, newly-opened ports and more.

Scan and retrieve OS data from Linux systems

It is possible to remotely extract OS data from Linux-based systems and scan results are presented in the same way as for Windows-based computers. This means that both Linux and Windows-based computers can be analyzed in a single scanning session! GFI LANguard N.S.S. includes numerous Linux security checks including rootkit detection. GFI LANguard N.S.S. can use SSH Private Key files instead of the conventional password string credentials to authenticate to Linux-based target computers.

System requirements

- Windows 2000 (SP4), XP (SP2), 2003, VISTA operating system
- Internet Explorer 5.1 or higher
- Client for Microsoft Networks component – included by default in Windows 95 or higher
- Secure Shell (SSH) – this is included by default in every Linux OS distribution pack.

Awards

Download your evaluation version from http://www.gfi.com/lannetscan/

GFI EventsManager

Event monitoring, management and archiving

The huge volume of system events that is generated daily is a valuable source of information for network administrators to help them monitor configuration changes, administrative actions, identify system errors and suspected security breaches. This is, however, an overwhelming task without the proper tools. The larger the network, the greater is your need for a solution that allows you to monitor, manage and archive thousands of events that are generated by devices across heterogeneous networks.

GFI EventsManager 8, an award-winning events monitoring, management and archiving solution, supports a wide range of event types such as W3C, Windows events, Sylogs and, in the latest version, SNMP traps generated by devices such as firewalls, routers and sensors. Providing support for devices from the top 20 manufacturers in the world as well as custom devices, GFI EventsManager allows you to monitor an extended range of hardware products, report on the health and operational status of each one and collect data for analysis. You can also track employee activity on the network such as changes made to their PCs, files accessed during the day, meet legal and regulatory compliance such as SOX, PCI DSS, HIPAA and much more.

- Information system and network security: Detect intruders and security breaches
- System health monitoring: Proactively monitor your servers
- Legal and regulatory compliance: An aid to meet regulatory compliance
- Forensic investigations: A reference point when something goes wrong.

Benefits

Why use GFI EventsManager?

- Centralizes Syslog, W3C, Windows events and SNMP Traps generated by firewalls, servers, routers, switches, phone systems, PCs and more
- Increase network uptime and identify problems through real-time alerting
- Fast and cost-effective monitoring and management of the entire network
- SQL Server Auditing for SQL Server 2000, 2005, 2008 and also MSDE & SQL Express
- Unrivaled event scanning performance scalable to over 6 million events per hour
- Certified for Windows Server 2008; Supports Windows Vista

Centralized event logging

Event logs are constantly and automatically generated by a user or by an automatic/background process and logs are often stored in disparate locations. GFI EventsManager stores all captured event logs into one SQL database that may also reside remotely. You may also configure scheduled backups of your event logs.

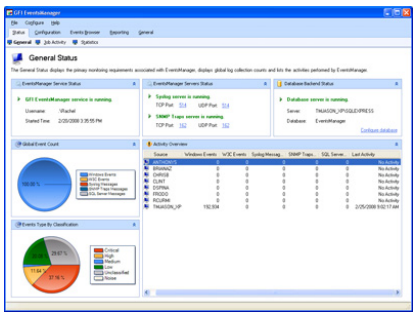
Analysis of event logs including SNMP Traps, Windows Event logs, W3C logs and Syslog

As a network administrator, you have experienced the cryptic and voluminous logs that make log analysis a daunting process. GFI EventsManager is a log processing solution that provides network-wide control and management of Windows event logs, W3C logs, and Syslog events generated by your network sources. GFI EventsManager now supports Simple Network Management Protocol version 3 which is the language spoken by low level devices such as routers, sensors, firewalls, etc. Through SNMP users can now monitor a whole range of hardware devices on their infrastructure with the ability to report on the health and operational status of each device.

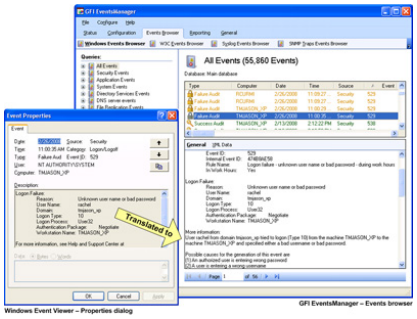
Certified for Windows Server 2008; Supports Vista

GFI EventsManager has achieved 'Certified for Windows Server 2008' status and can be installed on, and collect events from Windows Vista and Windows 2008. Although these new platforms use a different log format, GFI EventsManager presents events from various operating systems in the same manner, thus allowing the user to get used to a common structure, irrespective of the platform being monitored. GFI EventsManager also supports Windows 2000, Windows XP and Windows 2003.

GFI EventsManager



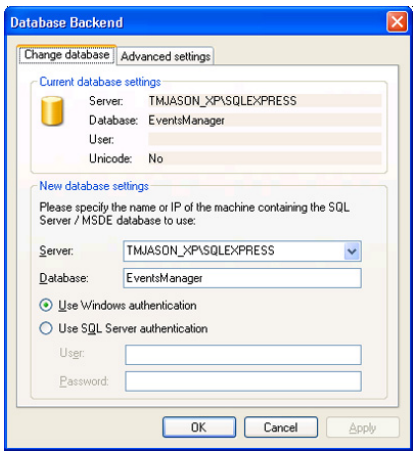
GFI EventsManager management console



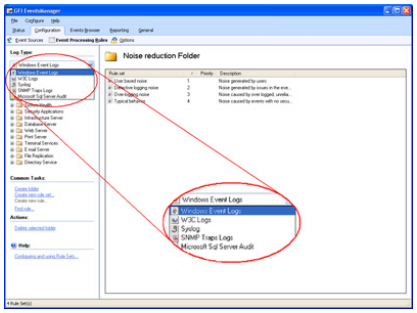
Windows Event Viewer – Properties dialog

GFI EventsManager – Events browser

Makes cryptic logs easier to understand

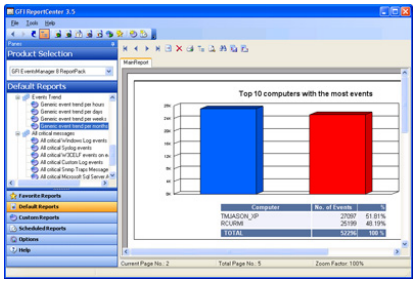


Centralized event logging



Support for multiple log types (Windows event logs, W3C, Syslog, SNMP Traps, Microsoft SQL Server audit)

GFI EventsManager ReportPack



Report showing Top 10 event-generating machines

Deeper granular control of events

GFI EventsManager helps you monitor a wider range of systems and devices through the centralized logging and analysis of various log types including Windows events, Syslog, W3C and now SNMP traps that are generated by network resources. Administrators can gather information from Windows machines and third-party devices at a greater level of granularity and also process information at extended tags level and base the decision on what to do with that information on the spot, without further information management.

Support for new Devices

Managing SNMP Trap for myriad devices requires the ability to understand the 'language' each manufacturers uses to define events. The definitions and device information are contained in Management Information Base (MIB) definition files which are provided by the manufacturers. GFI EventsManager ships with MIB definitions for the following vendors: Cisco, 3Com, IBM, HP, Check Point, Alcatel, Dell, Netgear, SonicWall, Juniper Networks, Arbor Networks, Oracle, Symantec, Allied Telesis and others. GFI EventsManager is also capable of importing the MIB files of new devices as soon as these become available.

SQL Server Auditing

GFI EventsManager now supports SQL server auditing for all commercial and free versions of SQL Server including 2000, 2005, 2008, MSDE and SQL Express. Auditing allows the user to track and report on SQL server activity such as: Running of SQL statements, altering DB tables, attempts to access data without necessary privileges, etc. This can ensure data in SQL servers is authentic and thus reliable.

"Translates" cryptic windows events

Cryptic logs make log analysis a lengthy process. GFI EventsManager "translates" the often cryptic event descriptions to clear, concise explanations and suggestions for action.

High performance scanning engine

GFI EventsManager incorporates a totally re-designed event scanning engine that is fine-tuned for maximum scanning performance. Tests demonstrate that it is able to scan and collect up to 6 million events/hr. Furthermore, its plug-in based methodology allows additional features and modules to be integrated without interfering with existing code.

Real-time alerts

GFI EventsManager can send you alerts when key events or intrusions are detected. You can trigger actions such as scripts or send an alert to one or more people by email, network messages, and SMS notifications sent through an email-to-SMS gateway or service.

Collect events data distributed over a WAN into one central database

You can collect events data from GFI EventsManager installations on multiple sites and locations across your network into a central database using the Database Operations functionality. This enables you to easily monitor thousands of workstations and servers across the network without impacting on bandwidth and storage use. It integrates and centralizes events collected and processed and allows you to backup/restore events on demand. Through database operations you can manage the size of the database – without the need for manual intervention – not only through centralization but by also being able to export events and back them up as needed.

Rule-based event log management

GFI EventsManager ships with a pre-configured set of log processing rules that allow you to filter and classify events that satisfy particular conditions. You can run these default rules without performing any configuration or you can choose to customize these rules or create tailored ones that suite your network infrastructure.

Advanced event filtering features

GFI EventsManager's powerful filtering sieves through the recorded event logs and allows you to browse the required events without deleting any records from your database backend. You may also selectively highlight specific events using a color or the integrated event finder tool.

Event log scanning profiles

Scanning profiles allow you to configure the set of event log monitoring rules that will be applied to a specific computer or to a group of computers and provide a centralized way of tuning event log processing rules. You can also setup a set of rules that only apply to workstations in a particular department. You may also create separate complementary profiles that provide additional and more specialized event log rules on a computer by computer basis.

View reports on key security information happening on your network

GFI EventsManager reporter, which ships with the product, allows you to create or customize reports, including standard reports, such as:

- Account usage reports
- Account management reports
- Policy changes reports
- Object access reports
- Application management reports
- Print server reports
- Windows event log system reports
- Events trend reports

Helps to comply with PCI DSS and other regulations

As from September 2007 all businesses handling cardholder data – irrespective of size – have to be fully compliant with strict security standards drawn up by the world's major credit card companies. Data logging is key to meeting PCI DSS requirements since logs provide audit trails of all activities in a credit card holder data environment and hence, a comprehensive log management system, such as GFI EventsManager, would provide you with the functionality you need to help you become PCI DSS compliant.

Other features:

- Remove "noise" or trivial events that make up a large ratio of all security events
- Real-time 24 x 7 x 365 day monitoring and alerting
- Graphically monitor the status of GFI EventsManager and your network through the built-in status monitor
- Report scheduling and automated distribution via email.

You're in good company...

Many leading companies have chosen GFI EventsManager. Here are just a few: Primerica, Pepsico France, Royal & Sunalliance USA Inc., ATP, Ceridian Canada and many more.

System requirements

- .NET Framework 2.0
- Microsoft Data Access Components (MDAC) 2.8 or later
- Access to MSDE / SQL Server 2000 or later

Awards

Download your evaluation version from http://www.gfi.com/eventsmanager/

GFI EndPointSecurity

Comprehensive control on use of iPods, USB drives and other portable devices

GFI EndPointSecurity allows administrators to actively manage user access and log the activity of:

- Media players, including iPods, Creative Zen and others
- USB drives, CompactFlash, memory cards, CDs, floppies & other portable storage devices
- PDAs, BlackBerry handhelds, mobile phones, smart phones and similar communication devices
- Network cards, laptops and other network connections.

How it works

To control access, GFI EndPointSecurity installs a small footprint agent on the machine. This agent is only 1.2 MB in size – the user will never know it is there. GFI EndPointSecurity includes a remote deployment tool based on GFI LANguard technology, allowing you to deploy the agent to hundreds of machines with just a few clicks. After installation, the agent queries Active Directory when the user logs on and sets permissions to the different nodes accordingly. If the user is not a member of a group that allows him/her access, then access to the device is blocked.

Benefits

Why choose GFI EndPointSecurity?

- Prevents data leakage/theft by comprehensively controlling access to portable storage devices with minimal administrative effort
- Prevents introduction of malware and unauthorized software on the network
- Gives administrators greater control by being able to block devices by class, file extensions, physical port or device ID
- Allows administrators to grant temporary device or port access for a stipulated time-frame
- Support for 32 & 64-bit platforms: Including Windows Vista and latest RC of Windows Server 2008.

Control user access and protect your network against the threats posed by portable storage media

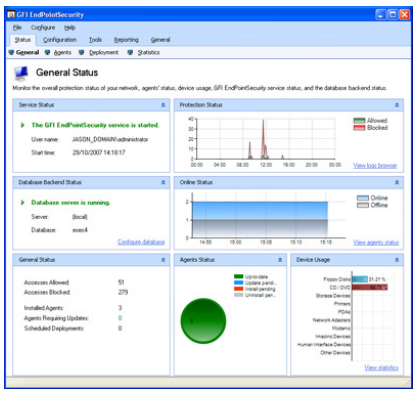
Using GFI EndPointSecurity you can centrally disable users from accessing portable storage media preventing users from stealing data or bringing in data that could be harmful to your network, such as viruses, trojans and other malware. Although you can switch off portable storage devices such as CD and/or floppy access from the BIOS, in reality this solution is impractical: You would have to physically visit the machine to temporarily switch off protection and install software. In addition, advanced users can hack the BIOS. GFI EndPointSecurity allows you to take control over a wide variety of devices including:

- Floppy disks
- CDs and DVD ROMs
- iPods
- Storage devices
- Printers
- PDAs
- Network adapters
- Modems
- Imaging devices
- And more!

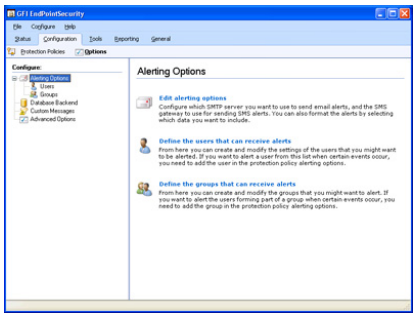
Log the activity of portable storage media like USB memory sticks, SD cards and more

USB sticks are one of the main threats as they are small, easily hidden and can store up to 4 GB of data. For example, plugging a digital camera into a USB port gives users access to storage on an SD card; SD cards are available in several sizes including 2 GB and over. In addition to blocking access to portable storage media, GFI EndPointSecurity logs device-related user activity to both the event log and a central SQL Server. A list of files that have been accessed (or read/written) on a device is recorded whenever a user plugs in a device to the network.

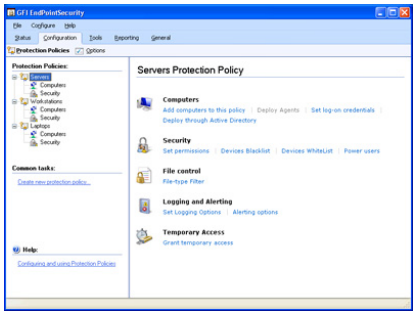
GFI EndPointSecurity



GFI EndPointSecurity Management Console

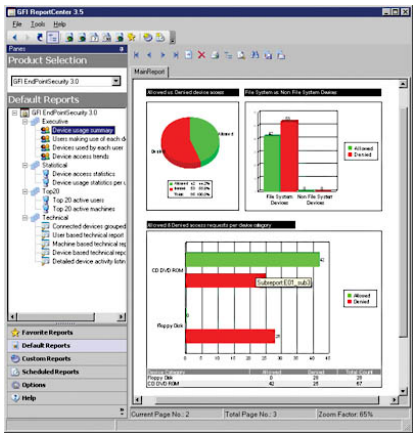


GFI EndPointSecurity configuration options



Default protection policies

GFI EndPointSecurity ReportPack



Device usage report

Easily configure group-based protection control via Active Directory

You can configure and categorize computers into different protection groups: For each group you may specify different levels of protection and devices to allow or disallow access to. You can also leverage the power of groups and make an entire department a member of the group and easily change the settings for the entire group. Configuration of GFI EndPointSecurity is effortless and leverages the power of Active Directory and does not require the administrator to remember and keep track of which policies were deployed to which computers. Other storage control software requires cumbersome per-machine administration, forcing you to make the changes on a per-machine basis and update the configuration on each machine before the settings can take effect.

Advanced granular access control, whitelists and blacklists

GFI EndPointSecurity enables you to allow or deny access to a range of device classes, as well as blocking files transferred by file extension, by physical port and by device ID (the factory ID that tags each device). It is also possible to specify users or groups that should always have full access to devices. GFI EndPointSecurity also allows administrators to define a device whitelist and blacklist to allow only company-approved devices and block all others.

Real-time status monitoring and real-time alerts

GFI EndPointSecurity provides real-time status monitoring through its user interface that displays statistical data through graphical charts, the live status of the agent and more. GFI EndPointSecurity also allows you to send alerts when specific devices are connected to the network. Alerts can be sent to one or more recipients by email, network messages, and SMS notifications sent through an email-to-SMS gateway or service.

Get full reports on device usage with the GFI ReportPack add-on

The GFI EndPointSecurity ReportPack is a full-fledged reporting add-on to GFI EndPointSecurity. This reporting package can be scheduled to automatically generate graphical IT-level and management reports based on data collected by GFI EndPointSecurity, giving you the ability to report on devices connected to the network, user activity endpoint files copied to and from devices (including actual names of files copied!) and much more.

Easy unattended agent deployment

GFI EndPointSecurity provides the possibility to administrators to automatically schedule agent deployment after the administrator makes policy or configuration changes. If a deployment fails, it is rescheduled until deployed successfully. Furthermore, the GFI EndPointSecurity remote deployment tool can deploy the agent network-wide in a few minutes. GFI EndPointSecurity allows Active Directory deployment through MSI.

Temporary device access

Temporary access can be granted to users for a device (or group of devices) on a particular computer for a particular timeframe. This can be done even if the GFI EndPointSecurity agent is not connected to the network!

Other features:

- Scan and detect a list of devices that have been used or are currently still in use
- Password protected agents to avoid tampering
- Set up custom popup messages for users when they are blocked from using a device
- Browse user activity and device usage logs through a backend database
- Maintenance function that allows you to delete information that is older than a certain number of days
- Support for operating systems in any Unicode-compliant language

You're in good company...

Many leading companies have chosen GFI EndPointSecurity. Here are just a few: Best Western Sterling Inn, Fair Trades Ltd, Central Highlands Water, Aurum Funds and many more.

System requirements

- Operating system: Windows 2000 (SP4), XP, 2003, Vista and 2008 (x86 and x64 versions)
- Internet Explorer 5.5 or later
- .NET Framework version 2.0
- Database Backend: SQL Server 2000, 2005, 2008
- Port: TCP port 1116 (default)

Awards

GFI NETWORK ServerMonitor

Network server monitoring software

GFI Network Server Monitor is a network monitoring software solution that enables administrators to scan the network for failures or irregularities automatically. With GFI Network Server Monitor, you can identify issues and fix unexpected conditions before your users (or managers) report them to you!

GFI Network Server Monitor maximizes network availability by monitoring all aspects of your Windows and Linux servers, workstations and devices (routers, etc). When a failure is detected, GFI's network monitor can alert you by email, pager or SMS, as well as taking corrective action by, for example, rebooting the machine, restarting the service or running a script.

GFI Network Server Monitor actually tests the status of a service, rather than deducing a service status from generated events (as other products do), which is the only real way to ensure server uptime! GFI Network Server Monitor is easy to set up and use, and is competitively priced.

GFI Network Server Monitor built-in monitoring rules include: Exchange Server 2000/2003, MS SQL, Oracle and ODBC databases, CPU usage, FTP & HTTP Servers Group Membership, Active Directory & NTDS, Disk Drive health, Disk Space, Event Log (with content checking), File Existence (with content checking), TCP, ICMP/Ping, SMTP & POP3 Mail servers, Printers, Processes, Services, UNIX Shell Scripts (RSH), SNMP & Terminal Server.

Custom monitor functions can also be created in VBscript and ADSI and WMI can also be leveraged, allowing you to monitor virtually anything!

Enterprise class architecture

GFI Network Server Monitor consists of a network monitoring service and a separate management interface. No agent software needs to be installed on the machines you wish to monitor. The Network Monitor Engine is multi-threaded and can run 40 checks at a time. This software architecture allows for high reliability and scalability to monitor both large and small networks.

Includes checks for Exchange 2000/2003, ISA server, IIS and others

Via the Quickstart wizard, you can quickly create a series of checks which monitor all the important services on your network, including Exchange Server, IIS and others. Critical Exchange services and performance counters (Information Store, mailboxes, SMTP service, etc) are monitored.

Benefits

Why choose GFI Network Server Monitor?

- Monitor your network and servers for software and hardware failures
- Out-of-the-box monitoring of Exchange, ISA, SQL, Web servers and more!
- Monitor disk space, services, processes, etc. on servers and workstations
- Easy to learn/use and easy to deploy – no client component/agent.

Monitors terminal servers by actually logging in

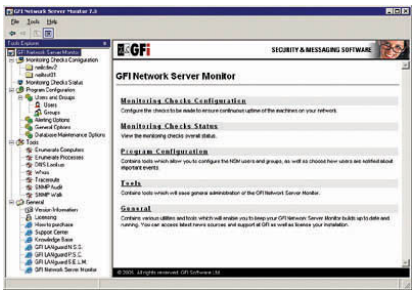
GFI Network Server Monitor can check the status of a terminal server by actually performing a complete login and checking if the session is established correctly. This monitoring method is superior to relying on the events that the terminal server generates (as Microsoft MOM does).

Monitor your database servers (SQL/ODBC)

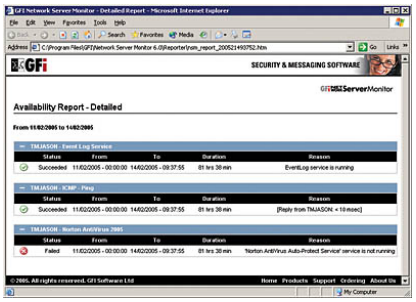
GFI Network Server Monitor can check the availability of all leading database applications. Out of the box, it can monitor Microsoft SQL Server via ADO. Other databases such as Access, FoxPro, Paradox, SyBase, Informix, IBM DB2 and many more can be monitored via ODBC.

Monitor Linux servers

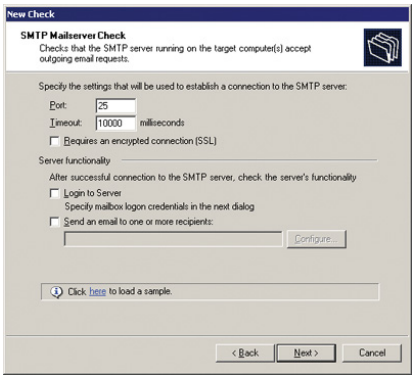
GFI Network Server Monitor includes extensive checks for monitoring Linux servers. You can monitor CPU usage, printer availability, file existence, process running, folder size, file size, users and groups membership, disk partition check and disk space. In addition, administrators can create any check by creating an SSH script.



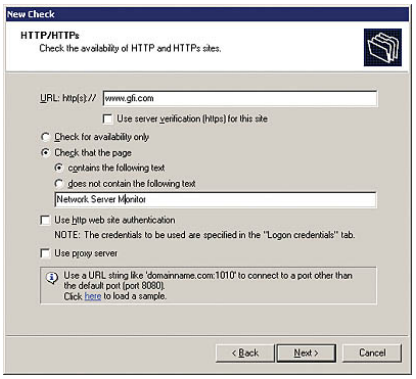
The GFI Network Server Monitor manager



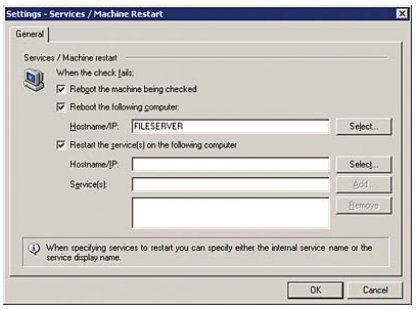
Detailed network resource availability report



Monitor SMTP server function



Monitor HTTP server function



Reboot or restart service upon failure detection

Performs administrative steps to ensure that a service is running

GFI has developed specialized checks which mimic administrator operations to verify that services offered by various applications are running, for example, logon to a service, perform a task and logoff the service – without the need for any administrative intervention! The monitoring functions that make use of such methodologies include: IMAP, POP3, SMTP Server and the email route check. Through the active use of such services one can guarantee that all aspects of these services are running and functioning.

Takes corrective action automatically

After an unexpected condition has occurred, GFI Network Server Monitor can automatically correct the problem by restarting a service (or multiple services) upon failure; rebooting a server upon failure; or launching an executable, batch job or VBScript.

Built-in computer monitor functions

- CPU usage function – Ensure that a processor's usage does not go beyond a certain level
- Performance counter – Monitor any internal operating system counter, including counters used by SQL Server and MSMQ
- Directory size function – Ensure that a particular directory (for example, a user's home directory) does not take up more than x amount of drive space
- Disk drive function – Monitor the physical status of the disk
- Disk space function – Check if sufficient disk space is available
- File existence function – Monitor the existence of a particular file, for example, results of scheduled batch jobs
- File size function – Monitor the size of particular files, for example, critical log files.

Built in Internet service functions

- HTTP function – Checks availability of HTTP and HTTPS sites; passes credentials if required
- Website content checking – Checks website content by specifying a text pattern
- FTP function – Checks availability of an FTP server/site
- ICMP ping function – Checks a remote host for availability
- IMAP server function – Checks that the IMAP service is functioning by logging into the service and checking the count of the emails contained in a specific folder on the IMAP server
- DNS server function – Checks DNS server by reading an 'A' record and verifying the result
- SMTP server function – Checks mail server by establishing a connection and handshaking to verify SMTP protocol is working correctly
- POP3 server function – Checks POP3 servers by establishing a connection and handshaking
- NNTP news server function – Checks connection and does a handshake
- SNMP function – Monitors specific variables on remote machines or devices via the SNMP GET message
- TCP port function – Checks if a port is responding and checks its response
- NTP timeserver function – Monitors status of timeservers
- Email route function – Checks the health of email services by actually sending test emails and verifying their delivery at destination. This check is also useful for verifying performance of your mailing systems
- Daemon function – SSH-based check that verifies if particular daemons are running on target Linux/Unix computer/s.

Alert notification via email, pager or SMS

When it detects a failure, GFI Network Server Monitor can send alerts via SMS, pager, email or a network message. SMS (text) messages are sent either through an SMS service provider (SMSC), directly through a connected GSM phone/modem; it is also possible to use the GFI FAXmaker email-to-SMS gateway service, Clickatell's web email-to-SMS online gateway service or any third party email-to-SMS gateway. All notifications can be customized using variables. Recipients can be configured globally for all rules.

Support for SQL Server/MS Access as a database backend

GFI Network Server Monitor allows you to store monitoring data to either an SQL Server or MS Access database backend. SQL Server is more appropriate for users with higher monitoring level requirements as well as those who need to centralize the monitoring results of multiple GFI Network Server Monitor installations in one place (such as backups, remote accessing as well as report generation by third party tools such as Crystal Reports or MS Reporting Services).

View network status from anywhere in the world

You can check rule status from any location using GFI Network Server Monitor's remote web monitor. The remote web monitor includes two types of web page views: One for a normal web browser and one optimized for viewing from a mobile phone or handheld device such as a BlackBerry or a Palm. A small footprint web server is included, although the feature can also be operated in conjunction with IIS.

Monitor remote event logs

GFI Network Server Monitor can scan Windows event logs on local or remote computers and look for specific event sources, categories, event IDs and patterns in the description of the event. In addition, it can look for multiple events occurring in a specific time interval, for example, a McAfee or Norton virus alert posted in the last 30 minutes.

Monitor processes, services performance and CPU usage

GFI Network Server Monitor enables you to check critical processes and services on local and remote computers. You can also monitor the CPU usage of a machine and any performance counter accessible through perfmon.msc. This way, you can ensure that virtually any application is running properly.

Custom network monitoring using VBScript and SSH

Although GFI Network Server Monitor includes an extensive set of default monitoring functions, you can build your own custom checks by writing a VBScript (Windows) or an SSH shell script (Linux). From VBScript, you can use both WMI and ADSI. WMI is an interface to a broad range of hardware/software/OS-related properties of a computer, allowing you to perform almost any check. Using ADSI, you can interface to Active Directory.

Monitor users, groups and other Active Directory information

Use GFI Network Server Monitor to monitor directory information. For example, monitor group membership of the domain admins group. You can also check user accounts (locked out, disabled, etc.), computer accounts, groups, group membership, organizational units, and so on.

Competitively priced

Network monitoring/management products are traditionally rather expensive. By contrast, GFI Network Server Monitor costs just USD 1,530 to monitor up to 50 IPs and USD 594 to monitor up to 10 IPs.

Nested folder support

It is possible to organize folders in a nested folder format - this provides support for more complex monitoring needs such as that of consultants or enterprises with more granular server distribution.

Other features

- Configure maintenance periods to avoid alerts being sent during scheduled maintenance
- Advanced logging options to text file or event log
- Configure dependencies to avoid multiple alerts for error conditions dependent on each other
- Monitor network printer status
- Reporting – includes reports that detail the availability of your network resources; alternatively, use Crystal Reports to access the database and create your own reports
- Monitoring checks wizard that easily configures new checks for your present systems
- Accommodates employee shifts: GFI Network Server Monitor can notify different people depending on the time at which the check triggered.

You're in good company...

Many leading companies have chosen GFI Network Server Monitor. Here are just a few: Manx Telecom Limited, ABC Fine Wine & Spirits, Satel 2000, The CBORD Group, Inc., and many more.

System requirements

- Windows 2000 (SP4 or higher), 2003 or XP Pro operating systems.
- Windows Script Host 5.5 or higher (included in Internet Explorer 6 and in Service Pack 2 of Internet Explorer 5.5; you can download it separately from http://msdn2.microsoft.com/en-us/library/ms950396.aspx.
- .NET Framework 1.1.

Download your evaluation version from http://www.gfi.com/nsm/

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.

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.

Features of GFI WebMonitor - UnifiedProtection Edition (common features)

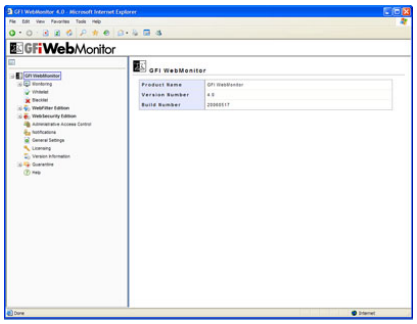
The features below are available with all editions.

Monitor or block a connection in real-time

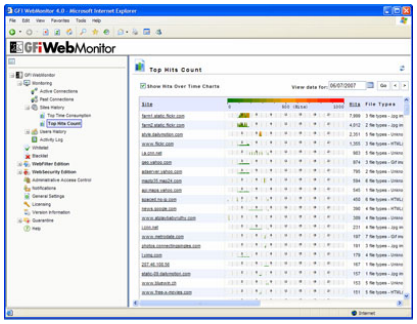
Administrators can see what websites the users are currently browsing and what files are being downloaded. An active connection, browsing session or download can be easily blocked by simply clicking on the block connection icon. For example, you may decide to interrupt the download of a large file that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

Monitor or block applications' hidden downloads

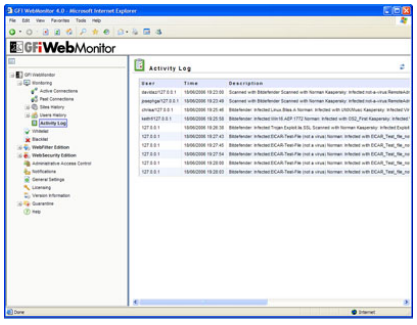
Some software applications automatically connect to their home pages to download updates using HTTP tunnelling. Although this can reduce administration, it can also present a security risk because unknown applications or trojans can use the same technique to download malicious files onto a user's PC, 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).



GFI WebMonitor main screen

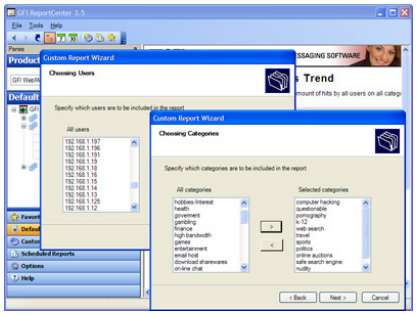


Monitors connections and provides statistics



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 is a leading software developer that provides a single source for network administrators to address their network security, content security and messaging needs. With award-winning technology, an aggressive pricing strategy and a strong focus on small-to-medium sized businesses, GFI is able to satisfy the need for business continuity and productivity encountered by organizations on a global scale. Founded in 1992, GFI has offices in Malta, London, Raleigh, Hong Kong and Adelaide which support more than 200,000 installations worldwide. GFI is a channel-focused company with over 10,000 partners throughout the world. GFI is also a Microsoft Gold Certified Partner. More information about GFI can be found at http://www.gfi.com.

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