GFI MailEssentials

for Exchange/SMTP

Anti-spam for Exchange, anti-phishing and email management

With fraudulent, inappropriate and offensive emails being delivered in vast quantities to businesses every day, anti-spam software is a vital component of your network security strategy. Spam wastes network users' time and network resources, and can also be dangerous. GFI MailEssentials offers anti spam for Exchange server and other email servers and eliminates the need to install and update anti-spam software on each desktop.

GFI MailEssentials offers a fast set-up and a high spam detection rate using Bayesian filtering 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 will eliminate over 98% of the spam from your network! GFI MailEssentials also detects and blocks phishing emails through a system of Uniform Resource Identifier (URI) and keyword checks. In addition to anti-spam filtering and anti-phishing protection, 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.

Features & benefits

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

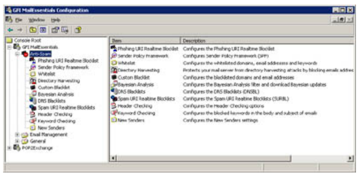
Allows users to review email marked as spam from junk mail folder

#1 server anti-spam solution @ unbeatable pricing: USD 450 (25), USD 1195 (100), USD 5000 (1000) mailboxes.

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:

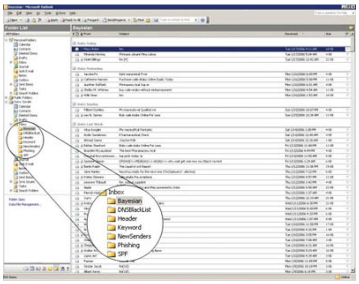
- Looks at the whole spam message, not just keywords or known spam signatures
- Learns from your outbound email (ham) and therefore greatly reduces false positives
- Adapts itself over time by learning about new spam and new valid email
- Dataset is unique to your company, making it impossible to bypass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

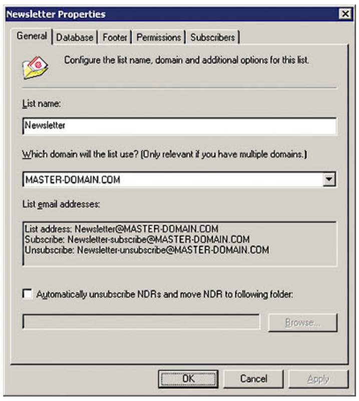


Item	Description
Phishing URI Realtime Blocklist	Configures the Phishing URI Realtime Blocklist
Sender Policy Framework	Configures Sender Policy Framework (SPF)
Whitelist	Configures the whitelisted domains, email addresses and keywords
Directory Harvesting	Protects your mail server from directory harvesting attacks by blocking emails addres
Custom Blacklist	Configures the blacklisted domains and email addresses
Bayesian Analysis	Configures the Bayesian Analysis filter and download Bayesian updates
DNS Blacklists	Configures the DNS Blacklists (DNSBL)
Spam URI Realtime Blocklists	Configures the Spam URI Realtime Blocklists (SURBL)
Header Checking	Configures the Header Checking options
Keyword Checking	Configures the blocked keywords in the body and subject of emails
New Senders	Configures the New Senders settings

GFI MailEssentials configuration



Users can review spam email



Configure the list name, domain and additional options for this list.

List name:

Newsletter

Which domain will the list use? (Only relevant if you have multiple domains.)

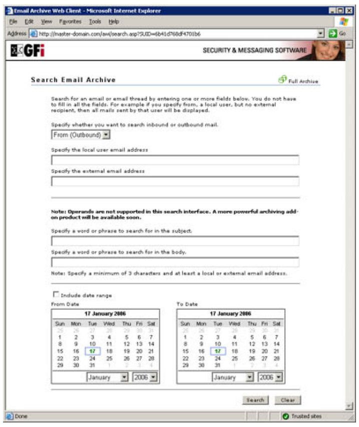
MASTER-DOMAIN.COM

List email addresses:

List address: Newsletter@MASTER-DOMAIN.COM
Subscribe: Newsletter-subscribe@MASTER-DOMAIN.COM
Unsubscribe: Newsletter-unsubscribe@MASTER-DOMAIN.COM

☐ Automatically unsubscribe NDRs and move NDR to following folder:

Newsletter list options


Email Archive Web Client - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address
Go
GFi
SECURITY & MESSAGING SOFTWARE
Full Archive

http://master-domain.com/awi/search.asp?SUID=6b41d768df4701b6

Search Email Archive

Search for an email or email thread by entering one or more fields below. You do not have to fill in all the fields. For example if you specify from, a local user, but no external recipient, then all mails sent by that user will be displayed.

Specify whether you want to search inbound or outbound mail.

From (Outbound)

Specify the local user email address

Specify the external email address

Note: Operands are not supported in this search interface. A more powerful archiving add-on product will be available soon.

Specify a word or phrase to search for in the subject.

Specify a word or phrase to search for in the body.

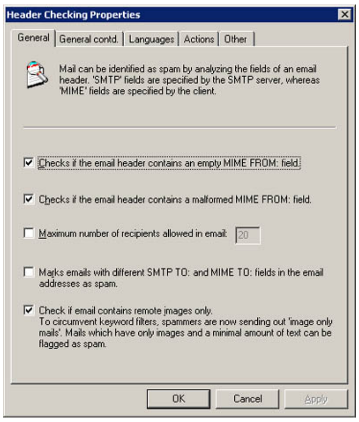
Note: Specify a minimum of 3 characters and at least a local or external email address.

☐ Include date range

From Date: 17 January 2006

To Date: 17 January 2006

Search email archive from anywhere via the web-based interface


Header Checking Properties
General | General contd. | Languages | Actions | Other

Mail can be identified as spam by analyzing the fields of an email header. 'SMTP' fields are specified by the SMTP server, whereas 'MIME' fields are specified by the client.

☑ Checks if the email header contains an empty MIME FROM: field.

☑ Checks if the email header contains a malformed MIME FROM: field.

☐ Maximum number of recipients allowed in email: 20

☐ Marks emails with different SMTP TO: and MIME TO: fields in the email addresses as spam.

☑ Check if email contains remote images only.
To circumvent keyword filters, spammers are now sending out 'image only mails'. Mails which have only images and a minimal amount of text can be flagged as spam.

Check email headers for spam practices

Protect your users against the menace of phishing emails

GFI MailEssentials provides the ability to detect and block threats posed by phishing emails through its Phishing URI Realtime Blocklist (PURBL). The GFI MailEssentials PURBL detects phishing emails by comparing Uniform Resource Identifiers (URIs) present in the email to a database of URIs which are known to be used in phishing attacks, and also by looking for typical phishing keywords in the URIs.

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.

Email header analysis & 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.

3rd 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 3rd 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.

Email monitoring

The email monitoring feature enables you to keep a central store of the email communications of a particular person or department. By configuring the mail to be copied to an email address, all email can be stored in an Exchange or Outlook store, making searching for email or content easy.

Email archiving to a SQL database

GFI MailEssentials can archive all inbound and outbound mail to a Microsoft SQL Server database. You can search for a particular email or an entire email thread via the included web interface. Mail archiving is essential for back-up and search reasons. For a complete email archiving solution, please check out GFI MailArchiver for Exchange.

Seamless integration with Exchange Server 2000/2003 & 5.5

GFI MailEssentials integrates seamlessly with Microsoft Exchange 2000/2003: 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 Notes and other popular SMTP/POP3 servers.

Content checking, anti-virus & 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.

Other features:

- Whitelisting of emails by keyword
- Blocking foreign language spam based on character set
- Email monitoring of particular user or department email communications
- Fake non-delivery reports (NDRs)
- Personalized server-based auto replies with tracking number
- POP3 downloader
- Web interface for searching email archive.

Reviews

Windows Server 2003 certification for GFI MailEssentials - GFI MailEssentials for Exchange/SMTP has achieved the Windows Server 2003 certification from Microsoft Corp through VeriTest. This certification is based on an established technical standard to identify software applications that are secure and manageable, and that run reliably on the Microsoft Windows family of operating systems. GFI MailEssentials met these rigorous requirements after being tested by VeriTest: "This certification through VeriTest provides GFI customers added confidence in their purchase of GFI MailEssentials," said Katrina Teague, Vice President of Marketing and Solutions at VeriTest.

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, 4, 5 or 5.5, Lotus Notes 4.5 and up, or an SMTP/POP3 mail server.
- For the list server feature, Microsoft Message Queueing Services is required.

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

GFI Software
Unit 2, St. John's Mews
St. John's Rd, Hampton Wick
Kingston-upon-Thames
Surrey KT1 4AN, 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 Software
Bargkoppelweg 72
22145 Hamburg
Germany
Tel +49(0) 40 3068 1000
Fax +49(0) 700 3068 1010
sales@gfisoftware.de

GFI Asia Pacific
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 05 Malta
Tel +356 21 382418
Fax +356 21 382419
sales@gfi.com

www.gfi.com