



# GFI MailEssentials

## for Exchange/SMTP/Lotus

Server-based anti-spam, anti-phishing, disclaimers & more

With fraudulent, inappropriate and offensive emails being delivered in vast quantities to businesses every day, spam protection is a vital component of your network's security strategy. Spam wastes network users' time and network resources, and can also be dangerous. GFI MailEssentials offers spam and phishing protection at server level 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 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 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 anti-spam involves training your users to create anti-spam rules sets, and subsequently users have to spend time updating these rules. Besides, such a system does not prevent your server message stores from filling up with spam.

### ■ Intelligent automatic whitelist management reduces false positives

Whitelists enable you to ensure that mail 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 mail recipients to your whitelist. This reduces false positives, without any need for additional administration. Whitelists can also be built based on domain names, email addresses and keywords.

#### Benefits

**Support for the industry leading messaging platforms including Microsoft Exchange 2000, 2003 and 2007**

**Highest spam detection rate (98+%) thanks to its Bayesian filtering technology**

**Lowest false positives through its patent pending auto whitelist feature**

**Server-based install, no client software required**

**Voted MExchange.org Reader's Choice Award Winner in the Anti-Spam category for four years.**

### ■ 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 mail (ham) and reduces false positives
- Adapts itself over time by learning about new spam and new valid mail
- Dataset is unique to your company, making it impossible to bypass
- Multilingual and international.

### ■ 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 emails, 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.

### ■ 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.

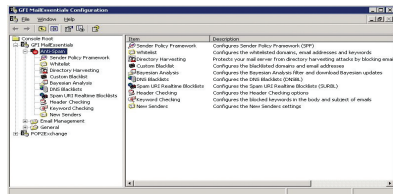
### ■ Support for SPF and multiple 3rd party SURBL servers

GFI MailEssentials' SPF module automatically checks whether the mail from a particular company was actually sent by its registered mail servers. GFI MailEssentials checks email content against SURBL servers; administrators can configure multiple SURBL servers, add their own and define the priority of which server must be checked first.



## Seamless integration with Exchange Server 2000/2003 & 5.5

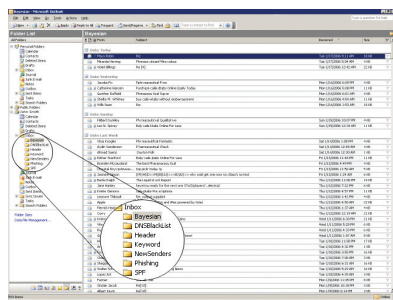
GFI MailEssentials integrates seamlessly with Microsoft Exchange 2000/2003: It installs on the Exchange SMTP service and does not require gateway configuration. Via the SMTP protocol, it also works with Exchange 5.5, Lotus Notes and other popular SMTP/POP3 servers.



GFI MailEssentials configuration

## 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). The GFI MailEssentials list server integrates with Exchange Server and can use Microsoft Access or Microsoft SQL Server as the backend. Both newsletter lists and discussion lists are supported.



Users can review spam mail



## 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 4.5 and up, or an SMTP/POP3 mail server.
- For the list server feature, Microsoft Message Queueing Services is required.

## 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 each 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.

## 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.

## Mail 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.

## Instant view of emails from new senders

The New Senders feature gives users an instant view of emails sent from people they never had previous contact with, helping them to better organize emails in their email client.

## 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.

## Reports on spam filtering and mail usage

The database-driven reporting engine allows you to create advanced reports on your inbound and outbound email, including the amount of spam filtered and which rules caught the most spam.

## 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.

## 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.

## 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.

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

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  
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 2138 2418  
Fax +356 2138 2419  
sales@gfi.com

Microsoft  
GOLD CERTIFIED  
Partner

  
www.gfi.com