G Data MailSecurity

General

Secure virus and spam protection for your email correspondence. *G Data MailSecurity* operates as a ***gateway*** independent from your ***mail server***; it can thus be combined with any mail server software within Windows or Linux and keeps your SMTP- or POP3-based correspondence safe from viruses, spam, phishing, and other threats - before they reach your server. We hope that your work with *G Data MailSecurity* is successful!

Your *G Data team*

Support frame

G Data MailSecurity is the software package for complete protection of your email traffic. The following support services complete the functionality of our software:

G Data PremiumHotline

The ***PremiumHotline*** for your *G Data Software* is available at any time for all registered business customers. .

www.gdata-software.com

Your ***registration number*** is located on the back of the user manual. If you have purchased the software online, the registration number is sent to you in a separate email. You can enter this via the ***online registration form*** and in this manner, you will then immediately be given a password online with which you can download your personal Internet updates. The ***Online database for frequently asked questions (FAQ)*** already contains answers to many questions concerning *G Data software.* Before contacting the ***hotline***, please check your computer/network configuration. The following information is particularly important:

- the ***version numbers*** of the administrator and ManagementServer (these can be found in the ***Help*** menu of the *G Data software*)
- the ***registration number*** or the ***user name*** for the ***Internet update***. The registration number is located on the back of the user manual. The user name is sent to you during ***online registration***.
- exact Windows version (Client/Server)
- other installed hardware and software components (Client/Server)

These details will make the call to the hotline representative faster, more effective and more successful. If at all possible, please ensure that the telephone is in the vicinity of a computer on which the Administrator software for the ManagementServer has been installed.

License agreements

The following are the contractual terms and conditions for the use of the *software* ***G Data MailSecurity*** by the end user (hereafter also called: Licencee).

1. Object of the contract: The object of the contract is the *G Data software* recorded on a data medium or downloaded from the Internet and the program description. This is hereafter referred to as Software. *G Data* calls attention to the fact that, due to the status of technology, it is not possible to manufacture Software in such a way that it operates without error in all applications and combinations.

2. Scope of use: *G Data* grants you, for the duration of this contract, the simple, non-exclusive and personal right (hereafter referred to as Licence) to use the Software on a contractually agreed number of computers. The Software can be used in the form of an installation on a physical unit (CPU), a virtual/emulated machine (such as VMWare) or an instance of a terminal session. If this computer is a multiple user system, this usage right applies to all users of this one system. As the Licencee you are permitted to transfer the Software from one computer to another in physical form (i.e. stored on a data medium), provided that it is not used on more than the contractually agreed number of computers at any time. Use that exceeds this is not permitted.

3. Specific limitations: The Licencee is prohibited from changing the Software without the prior written consent of *G Data*.

4. Ownership of rights: When purchasing the product you only receive ownership of the physical data medium onto which the Software has been recorded and to updates agreed in the context of support. Purchase of rights to the Software itself is not included with this. *G Data* especially reserves all publication, reproduction, processing and usage rights to the Software.

5. Reproduction: The Software and associated written materials are protected by copyright. Creation of a backup copy is permitted, as long as this is not passed on to a third party.

6. Duration of the contract: The contract is granted for an unspecified period. This duration does not cover the procurement of updates. The Licencee's right to use the Software expires automatically and irrevocably if he breaches any of the terms of this contract. On termination of the usage right it is obligatory that the original CD-ROM including any UPDATES/UPGRADES and any written materials is destroyed.

7. Compensation for breach of contract: *G Data* calls attention to the fact that you are responsible for all damages through breach of copyright that *G Data* incurs from breach of the terms of this contract by you.

8. Changes and updates: Our most recent service terms and conditions shall always apply. The service terms and conditions may be changed at any time, without notice and without giving reasons.

9. *G Data* warranty and liability:

a) *G Data* guarantees with respect to the original Licencee that, at the time of delivery, the data carrier (CD-ROM) onto which the Software has been recorded is error-free under normal conditions of use and within normal maintenance conditions for material performance.

b) If the data medium or download from the Internet is faulty, the purchaser is entitled to demand delivery of a replacement during the warranty period of 6 months from delivery. To do so, he must provide proof of purchase of the Software.

c) As per the reason previously stated in para. 1, *G Data* accepts no responsibility for the Software not being error-free. In particular, *G Data* accepts no warranty for the Software meeting the purchaser's requirements and purposes or working in conjunction with programs selected by him. The purchaser is responsible for proper selection and consequences of use of the Software, together with its intended or achieved results. The same is true of written materials related to the Software. If the Software is essentially unusable in the sense of section 1, the purchaser has the right to revoke the contract. *G Data* has the same right if manufacture of Software that may be required in the sense of para. 1 is not possible within reasonable cost limits.

d) *G Data* is not liable for damages unless damage is caused intentionally or by gross negligence on the part of *G Data*. Liability for gross negligence does not extend to sales persons. The maximum award for damages shall be the purchase price of the Software.

10. Legal domicile: The exclusive legal domicile for all disputes directly or indirectly arising from this contract is the registered head office of *G Data*.

11. Final provisions: If individual provisions of this Licence Agreement become invalid, the remaining provisions stay in force. In place of the invalid provision, an effective provision that approximates its commercial intention as closely a possible shall be considered as agreed upon.

Prior to installation

G Data MailSecurity is the software package for complete protection of your email communication. It comprises:

- ***G Data MailSecurity MailGateway***: The *MailGateway* is high end virus protection for your email correspondence and thus efficiently and securely blocks the main path for spreading the latest viruses. It operates as a gateway independent of your mail server and can thus be combined with any mail server software under Windows as well as Linux.
- ***G Data MailSecurity Administrator***: Control software for the MailGateway.

The program is a mail gateway for SMTP and POP3 with integrated virus protection.

- ***SMTP***: Incoming email is no longer sent to the mail server but to *G Data MailSecurity MailGateway*. After the virus scan, email is forwarded to the mail server from there. *G Data MailSecurity* can naturally also check outgoing email. To do so, the mail server is configured so that it no longer sends email directly but forwards it to *G Data MailSecurity* first. The program then takes care of further processing.
- ***POP3***: You can also use *G Data MailSecurity* if you retrieve your email using POP3. *G Data MailSecurity* retrieves the emails on behalf of the requesting program, checks them for viruses and then forwards them to the program.

Before the installation you should, of course, think about where you install *G Data MailSecurity* in the network. While you can use the *G Data MailSecurity Administrator software* from any point in the network, the installation of the actual MailGateway requires some prior consideration. In general, the MailGateway should ideally be located directly behind your network firewall (if you are using one), that is, the SMTP/POP3 data stream from the Internet via the ***firewall*** is sent directly to the MailGateway and distributed from there.

? Please note that you might have to change your ***firewall configuration*** (IP address and/or port) so that email traffic is processed using the *G Data MailSecurity MailGateway*.

In principle, you can install the *G Data MailSecurity MailGateway* on a separate computer, which then acts as the mail gateway for the entire network, but you can also use *G Data MailSecurity* on the computer that also acts as a mail server. In doing so, you need to keep in mind that installing both of them on a single computer can cause delays in the event of heavy email traffic because the administration of permanent email communication as well as the immanent virus scan are very resource intensive operations.

Installation of MailGateway on the mail server (SMTP)

If your ***SMTP server*** allows you to change the port number, you can also install *G Data MailSecurity* on the same computer as your SMTP server. In this case, please assign a new port number (e.g. 7100 or above) to your original mail server. The *MailGateway* then continues to use ***port 25*** to process incoming email.

? If you install *G Data MailSecurity* on the same computer as ***Microsoft Exchange 5.5***, then *G Data MailSecurity Setup* can automatically change the port for incoming email.

To do so, the SMTP entry in the ***\winnt\system32 \drivers\etc\services*** file is changed and the Microsoft Exchange Internet mail service is restarted.

Example:

Mail server configuration

- Port for incoming email: 7100 (example)
- Message transfer: Forward all messages to host: 127.0.0.1

Configuration of G DATA MailSecurity MailGateway (Incoming (SMTP))

- Port at which email is received: 25
- Use DNS to send email: OFF
- Forward email to this SMTP server: 127.0.0.1
- Port: 7100 (example)

Configuration of G DATA MailSecurity MailGateway (Outgoing (SMTP))

- Process outgoing email: ON
- IP addresses of servers that can send outgoing email: 127.0.0.1; <IP mail server>
- Use DNS to send email: ON

Terms

- <IP mail server> = IP address of the computer on which the mail server is installed.
- <IP G Data MailSecurity> = IP address of the computer on which G Data MailSecurity is installed

Installation of MailGateway on a separate computer (SMTP)

Here, incoming email must be sent to the *G Data MailSecurity MailGateway* (not to the mail server). This can be achieved in a number of ways:

a) Adjust the ***MX record*** in the ***DNS entry***

b) Define redirection to the ***firewall*** (if available)

c) Change the ***IP address*** of the mail server and assign the computer with the *G Data MailSecurity MailGateway* the original IP address of the mail server

? ***Mail server configuration***

- Port for incoming email: 25
- Message transfer: Forward all messages to host: <IP G Data MailSecurity>

Configuration of G Data MailSecurity MailGateway (Incoming (SMTP))

- Port at which email is received: 25
- Use DNS to send email: OFF
- Forward email to this SMTP server: <IP mail server>
- Port: 25

Configuration of G DATA MailSecurity MailGateway (Outgoing (SMTP))

- Process outgoing email: ON
- IP addresses of servers that can send outgoing email: <IP mail server>
- Use DNS to send email: ON

Terms

- <IP mail server> = IP address of the computer on which the mail server is installed.
- <IP G Data MailSecurity> = IP address of the computer on which G Data MailSecurity MailGateway is installed

System requirements

To use *G Data MailSecurity*, the following hard disk space is required:

- Mail Gateway: 20 MB plus temporarily stored email (recommended: at least 50 MB free)
- Administrator: 2 MB
- Prerequisites for using *G Data MailSecurity Administrator*: Pentium PC with Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2 operating system, 32 MB RAM
- Prerequisites for *G Data MailSecurity MailGateway*: Pentium PC with Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2 operating system, 256 MB RAM, CD-ROM drive, Internet access

? *G Data MailSecurity* can also run on 64 bit Windows operating systems.

Installation

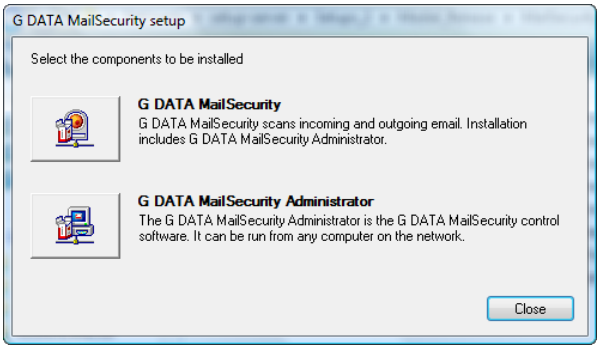
Please close all other programs before beginning to install *G Data MailSecurity*. Errors or termination could occur if, for example, programs are left open that access data that *G Data MailSecurity* requires for the installation. Please make sure that there is sufficient hard disk space in your system for the installation. If there is insufficient memory available during the installation, *G Data MailSecurity* will notify you of this.

The installation of *G Data MailSecurity* is markedly straightforward. Simply start Windows and place the *G Data MailSecurity CD-ROM* in your CD-ROM drive. An installation window opens automatically, offering the following options:

- **Install**: Use this to begin installing *G Data MailSecurity* on your computer.
- **Browse**: Here you can view the *G Data MailSecurity CD-ROM* directories using Windows Explorer.
- **Cancel**: Clicking on this will let you close the Autostart window without having to perform any actions.

? If you have not activated the ***Autostart function for your CD-ROM drive***, *G Data MailSecurity* will not be able to start the installation process automatically. In the Windows ***Start menu***, click ***Run***, enter ***e:\setup.exe*** in the window displayed and click ***OK***. This will then open the welcome screen for *G Data MailSecurity installation*. The ***e:*** signifies the drive character designation of your CD-ROM drive. If your CD-ROM drive is set up under a different drive character designation, please enter the relevant letter instead of ***e:*** .

All you have to do now is follow the individual steps of the installation wizard and use the **G Data MailSecurity** button to install the MailGateway on the computer you wish to use for this purpose. Ideally, this can be a dedicated MailGateway computer but it can also be the mail server computer itself or any other computer in the network that can perform administrative tasks. In this regard, please keep in mind the ***minimum system requirements*** for operating the MailGateway.


G DATA MailSecurity setup
Select the components to be installed
G DATA MailSecurity
G DATA MailSecurity scans incoming and outgoing email. Installation includes G DATA MailSecurity Administrator.
G DATA MailSecurity Administrator
The G DATA MailSecurity Administrator is the G DATA MailSecurity control software. It can be run from any computer on the network.
Close

G Data MailSecurity MailGateway

After completing the installation, the *MailGateway software* is available. Aside from the actual software, which runs in the background, the ***Administrator***, which gives you full access to the functions and options of the MailGateway, was installed automatically. This administrator can be found under ***Start > Programs > G Data MailSecurity > G Data MailSecurity*** with a standard installation. The settings and authority options provided by the Administrator are described in detail in the following sections.

? You can also maintain the MailGateway via any other computer that meets the system requirements for the *G Data MailSecurity Administrator tool*. Therefore, if you want to control the MailGateway using another computer in the network, you simply install the Administrator there without the actual MailGateway software. To do this, simply start the setup and choose the ***G Data MailSecurity Administrator*** button.

? If you close the administrator software, the MailGateway will not close. This continues to remain active in the background and controls the processes that were run by you.

Sending and receiving ***email*** is generally controlled using the ***SMTP*** and ***POP3*** protocols. Here, SMTP (= Simple Mail Transfer Protocol) is used to send email to any recipient whereas POP3 (= Post Office Protocol 3), as a higher-level protocol, is used to store received email in a special *mailbox*, which can only be accessed by the respective recipient by means of a password. Depending on how your network is set up, *G Data MailSecurity* can now use various node points to check incoming email for virus infections:

- If you are using an ***SMTP server*** in your network, *G Data MailSecurity* can check incoming email even before it reaches the mail server. The **Check incoming email (SMTP)** function is available in the ***Status area*** for this.

- If you receive your email directly from an external server as ***POP3 email*** (e.g., via a ***POP3 collective account***), *G Data MailSecurity* can also work here, and check the POP3 email for viruses before opening by the recipient. The **Scanning incoming email (POP3)** function is available in the ***Status area*** for this.

Of course, *G Data MailSecurity* can also scan all your outgoing email for virus infections before it is sent to the recipient. Since only the SMTP protocol is used for sending email, there is naturally no POP3 variant for this. You can use the **Scanning outgoing email (SMTP)** function in the ***Status area*** for this.

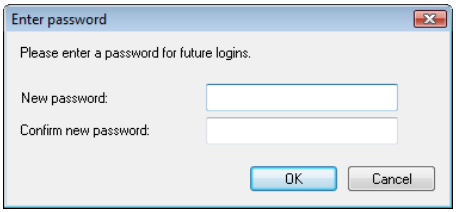
G Data MailSecurity Administrator

The *G Data MailSecurity Administrator* is the administration software for the *G Data MailSecurity MailGateway*, which protects all the SMTP- and POP3-based email traffic with and within your entire network and is centrally controlled by the system administrator. The ***Administrator*** can be started from any computer running Windows, using password protection. All possible changes to the virus scanner and virus signature update settings can be performed as remote-controlled jobs.

Initial program start (password assignment)

You can use the ***AdministratorTool*** to control the mail gateway by clicking on the entry ***G Data MailSecurity Administrator*** in the program group ***Start > (All) Programs > G Data MailSecurity*** in the start menu. When you start the Administrator, you will be asked for the server and password.

In the **Server** field, enter the computer name or the IP address of the computer on which the MailGateway has been installed. Since no **password** has been assigned yet, simply click the **OK** button without entering a password. A password entry window now opens in which you can enter a new password for the *G Data MailSecurity Administrator* under **New password**.

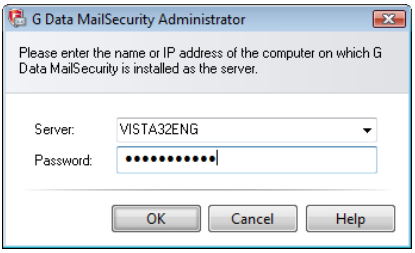


Confirm the entered password by typing it again in the **Confirm new password** field and then clicking **OK**.

? In the **Options** area of the **Advanced** tab, you can reassign the password by clicking the **Change password** button at any time.

Other program starts (access password)

You can use the AdministratorTool to control the mail gateway by clicking on the entry ***G Data MailSecurity Administrator*** in the program group ***Start > (All) Programs > G Data MailSecurity*** in the start menu. When you start the Administrator, you will be asked for the server and password.



In the **Server** field, enter the computer name or the IP address of the computer on which the MailGateway has been installed.

Administrator program areas

Use of *G Data MailSecurity* is generally self-explanatory and clearly structured. Using various tabs selected via the icons displayed on the left hand side of the *G Data MailSecurity Administrator* screen, you can select the relevant program area where you can carry out different actions, select default settings or review processes. The following program areas are available:


Status


Filters


Queues


Activity


Virus results

Additionally, you can find overlapping functions and settings in the menu bar at the top of the program interface.


Options: Here you can change the basic settings for operating *G Data MailSecurity* to meet your individual requirements.


Spam filter: The spam filter provides you with an extensive range of settings options for effectively blocking email with undesirable content or from undesirable senders (e.g., mass email senders).


Update: In the Internet update area, you can create basic settings for automatically downloading current virus signatures from the Internet. You can schedule these downloads according to your individual requirements and also update the *G Data MailSecurity* program files.

Virus encyclopaedia: This button connects you directly to the large ***AntiVirusLab virus encyclopaedia*** (***www.antiviruslab.com***). This comprehensive online encyclopaedia contains information about current viruses and offers an extensive archive, which explains already known viruses and their malicious functions in detail.

Help: Here you can access the online help for the product.

Info: This is where you get information about the program version.

Status

In the Administrator Status area, you will find basic information about the current status of your system and the MailGateway. This information, consisting of text, figures or dates, is displayed to the right of each item.

As long as your *G Data MailSecurity* is optimally configured for protection from computer viruses, you will see a green traffic light icon to the left of the listed entries.

If a component is not optimally set (e.g., obsolete virus signature or switched off virus check), a warning icon will alert you.

By double-clicking the relevant entry (or by selecting the entry and clicking the **Edit** button), you can directly select actions here or switch to the relevant program area. As soon as you have optimised the settings for a component with a warning icon, the icon in Status area will revert to the green traffic light icon. The following entries are available

- **Process incoming email**: Processing incoming email ensures that email is checked by the MailGateway before being forwarded to the recipient. If you double-click this entry, the corresponding settings window appears (menu bar: ***Options*** **>** ***Incoming (SMTP)***) and you can configure incoming email processing to your individual requirements.
- **Virus scan for incoming email**: Scanning incoming email stops infected files from reaching your network. If you double-click this entry, the corresponding settings window appears (menu bar: ***Options*** **>** ***Virus check***) and you can configure incoming email scanning to your individual requirements.

- **Process outgoing email**: Processing outgoing email ensures that email is checked by the MailGateway before being forwarded to the recipient. If you double-click this entry, the corresponding settings window appears (menu bar: ***Options*** > ***Outgoing (SMTP)***) and you can configure incoming email processing to your individual requirements.
- **Virus scan for outgoing email**: Scanning outgoing email stops infected files from being sent from your network. If you double-click this entry, the corresponding settings window appears (menu bar: ***Options*** > ***Virus check***) and you can configure outgoing email scanning to your individual requirements.
- **OutbreakShield**: ***OutbreakShield*** lets you detect and neutralise malware in mass mail before the updated signatures are available for this purpose. OutbreakShield uses the Internet to monitor increased volumes of suspicious email, enabling it to close the window between the mass email outbreak and its containment with specially adapted signatures, almost in real time.
- **Automatic updates**: The virus signatures can be updated separately. In general, you should enable the automatic ***updates*** option. If you double-click this entry, the corresponding settings window appears (menu bar: ***Internet update***) and you can configure the update frequency to your individual requirements.
- **Date of virus signatures**: The more current your virus signatures, the more secure your virus protection is. You should update the ***virus signatures*** as often as possible and automate this process, if possible. If you double-click this entry, the corresponding settings window appears (menu bar: ***Internet update***) and you can also perform an Internet update directly (irrespective of possible schedules).
- **Spam filter**: The ***Spam filter*** offers extensive settings options which effectively block email with unwanted content or email from unwanted senders (e.g. mass email senders).
- **Spam OutbreakShield**: The ***Spam OutbreakShield*** can detect and eliminate mass email quickly and safely. Before email is retrieved from the Internet, Spam OutbreakShield queries particular increased volumes of suspicious email and does not even let them reach the recipient's inbox.

Filters

In the Filter area you can use convenient filters to block incoming mail or automatically remove potentially dangerous content from email.

The respective filters are shown in the list under Filters and can be enabled or disabled as required by selecting the checkbox to the left of the respective entry. If you see a check in the checkbox, it means that that filter is active. If there is no checkmark in the box, the filter is inactive.

- **Import**: You can also save individual filters with your special settings as an XML file and, if necessary, reuse them or use them on other computers.
- **Export**: You can also save individual filters with your special settings as an XML file and, if necessary, reuse them or use them on other computers. To export more filters, select these with the mouse and at the same time hold the ***Ctrl key***.
- **New**: You can create new filter rules with the **New** button. When you create a new filter, a selection window appears in which you can specify the basic filter type. All of the other details about the filter can be created using a wizard, which will guide you through that filter type. This is a convenient way to create filters for every imaginable type of threat.
- **Edit**: You can edit existing filters with the **Edit** button.
- **Delete**: To permanently delete a filter, click the relevant filter once to highlight it and then click the **Delete** button.
- **Statistics**: You can invoke statistical information for every filter.
- **Protocol**: For the ***spam filter*** there is a log with a list of emails rated as potential spam. The log also shows which criteria were responsible for the spam rating (spam index values). In the event of an incorrect spam rating, you can inform the OutbreakShield server online that there has been a false detection (*false positive*) here . The mail is then rechecked by OutbreakShield and - if it really was falsely detected as spam - it is then reclassified as harmless. ***Warning***: In doing so, only a checksum is transferred and not the content of this email.

? Of course, your network is also protected from virus infections, irrespective of individual filter rules because *G Data MailSecurity* continuously checks incoming and outgoing mail in the background. Filter rules are thus designed to protect your email accounts from unsolicited mail, spam and unsafe scripts, and to minimise potential viruses sources even before the actual virus detection by *G Data MailSecurity*.

? ***General filter functions***

For all filter types you can generally enter a definitive name for the filter under **Name**; the filter will then be displayed in the filter list with this name, and you can specify internal notes and comments for the filter concerned under **Note**. Under **Direction** you can specify, in general, whether a filter rule is supposed to apply only to ***incoming email***, only to ***outgoing email***, or both directions.

? ***Reaction***

In the **Reaction** section, you can specify how email should be handled as soon as it meets the filter criteria, in other words, as soon as they were defined as spam.

You can thereby customise the text for the functions **Notify sender** and **Send alert to the following persons**.

To do so, simply click the ••• button to the right of the respective reaction. You can also use wildcards here to copy the information relating to the rejected email into the notification text.

In the text you define for the **Subject** and the **Email text**, the following **wildcards** (defined using a percentage symbol followed by a lower case letter) are available:

- %s ***Sender***
- %r ***Recipient***
- %c ***Cc***
- %d ***Date***
- %u ***Subject***
- %h ***Header***
- %i ***Sender IP***

The different filter types are explained in detail in the sections below:

Filter read receipt

This filter deletes requests for a read receipt. This is a reply email that is sent automatically as soon as the recipient has read an email with a read receipt request.

Disable HTML scripts

This filter disables scripts in the HTML part of an email. Scripts that might look OK on a web page tend to be rather irritating when they are integrated into an HTML email. In some cases, HTML scripts are also used to actively infect computers, whereby scripts have the option of running not only when the infected attachment is opened but even in an ***email preview***.

Disable external references

Many newsletters and product announcements in ***HTML email format*** contain links, which are only executed and displayed if the email is opened. These can be, for example, images that were not sent with the email but retrospectively loaded automatically via a ***hyperlink***. Since not all of these are just *harmless* graphics but can also be malicious routines, it makes sense to disable these references. Disabling them does not affect the actual email text.

Filter attachments

A large selection of filter choices for filtering ***email attachments*** and enclosures are provided. Most email viruses are spread through attachments, which usually have more or less well-hidden executable files. This can be in the form of a standard EXE file, which includes malware, but also VB scripts, which could be hidden behind apparently safe image, film or music files. In general, users should exercise extreme caution when opening email attachments. If in doubt, the sender of the email should be asked before opening files that have not been expressly requested.

Under **File extensions** you can list the file endings to which you would like to apply the respective filter. This lets you summarise all executable files (e. g. EXE and COM files) in one filter, and have another filter for other formats (e.g. MPEG, AVI, MP3, JPEG, JPG, GIF, etc.) if their file size would overload the mail server. You can also filter ***archive files*** (e.g. ZIP, RAR or CAB) . Please separate all file extensions in a filter group by a semicolon, e. g., **.exe*; **.dll*.

Under Mode, indicate whether you would like to allow the file endings under File extensions (**Only allow specified attachments**) or prohibit them (**Filter specified attachments**).

The function **Also filter attachments in embedded email** ensures that the filtering performed under **File extensions** for the selected attachment types also applies to email messages that are themselves being forwarded as email attachments. This option should normally be activated.

Choosing **Only rename attachments** has the effect that attachments that are to be filtered are not deleted automatically but only renamed. This is not only recommended for executable files (such as EXE and COM) but also for Microsoft Office files that may contain executable scripts and macros. Renaming an attachment makes it impossible to open it simply by clicking it. Instead, the user must first save (and possibly rename) the attachment before it can be used. If the checkmark for the **Only rename attachments** function has not been set, the respective attachments are deleted directly.

Under **Suffix**, you can enter a character string with which the actual file extension should be extended; in this manner, the execution of a file by simple clicking is prevented (**.exe_danger*, for instance).

Under **Insert message in email text** you can inform the recipient of the filtered email that an attachment was deleted or renamed based on a filter rule.

Content filter

You can use the content filter to easily block email that contains certain subjects or text. To do this, under **Regular expression** simply enter the keywords and expressions that *G Data MailSecurity* should respond to and under **Search scope** specify which parts of an email are to be scanned for these expressions.

You can use the **New** button on the right of the input field for **Regular expression** to conveniently enter text that triggers a filter action. It is possible to use the logical operators***AND*** and ***OR*** to link text components with one another.

? For example, if you enter *alcohol* ***AND*** *drugs*, the filter would be activated with an email that, for instance, has the terms*alcohol* and *drugs*, but not with an email that only has the term *alcohol* or only the term *drugs*. The ***AND*** logical operator requires that all components that have been linked with ***AND*** be present, while the ***OR*** operator requires that at least one of the elements be present.

You can also combine any **search terms** of your choice without the input help under Regular expression. To do so, simply enter the ***search terms*** and link them using a logical operator:

OR	corresponds to the ***vertical line***	(AltGr + <)	|
AND	corresponds to the ***ampersand***	(Shift + 6)	&

Sender filter

You can use the sender filter to easily block email coming from certain senders. To do this, under **Addresses/Domains**, simply enter the email addresses or domain names to which *G Data MailSecurity* should respond. Use a semicolon to separate multiple entries.

? You can also automatically filter out email with no sender.

Recipient filter

You can use the recipient filter to easily filter emails for certain recipients. To do this, under **Addresses/Domains**, simply enter the email addresses or domain names to which *G Data MailSecurity* should respond. Use a semicolon to separate multiple entries.

? You can also automatically filter out emails with a blank recipient field (i.e. emails that only have Bcc and/or Cc recipients).

Filter spam

The spam filter provides you with an extensive range of settings options for effectively blocking email with undesirable content or from undesirable senders (e.g. mass email senders). The program checks for numerous email characteristics that are typical of spam. These characteristics are used to calculate a value reflecting the likelihood of it being spam. To this end multiple tabs are available providing you with all the relevant settings options sorted by subject. The function and settings options of the spam filter are explained in detail in the chapter ***Spam filter***.

IP filter

The IP filter prevents the receipt of email sent from certain servers. Here, under **Name** and **Note**, enter information about why you want to block the respective IP addresses and then enter every individual IP address under **Do not accept email from the following IP addresses**. Click **Add** to add the IP address currently being entered to the list of blocked IP addresses.

? You can also export the list of IP addresses as a txt file or import a relevant txt list with IP addresses.

Language filter

The language filter lets you automatically define email in specific languages as spam. For example, if you do not generally have email contact with a German-speaking person, then you can set *German* as a spam language which should be filtered out. Simply select the languages in which you do not receive regular email contact and *G Data MailSecurity* will significantly raise the spam probability for such emails.

Queues

The Queues area always provides an overview of incoming and outgoing email accumulated in the MailGateway and being scanned for viruses and/or content. Email is usually forwarded immediately, only delayed minimally by the MailGateway and then immediately deleted from the queue list. If an email cannot be delivered or there are delays in the delivery (e.g. because the respective server is not responding), a corresponding entry is made in the queue list. *G Data MailSecurity* then tries to resend the email at intervals that can be set (under ***Options >*** ***Queue***). An email delivery that did not take

place or has been delayed is thus always documented. Use the **Incoming/ outgoing** button to switch from the ***List view for incoming email*** to the ***List view for outgoing email***. The **Repeat now** button enables you to re-deliver a selected email that could not be sent - irrespective of times that you have specified for the repeated delivery under ***Options > Queue***. The **Delete** button lets you permanently remove email that cannot be delivered from the queue.

Activity

The activity area provides a summary of the actions carried out by *G Data MailSecurity* at any time. These are listed with the ***time***, ***ID*** and ***action description*** in the activity list. You can use the scrollbar on the right to scroll up and down in the log. The **Reset** button allows you to delete the log created up to then and *G Data MailSecurity* starts recording the activities anew. With the function **Deactivate scrolling**, the list will continue to be updated, but the most recent activities will not be directly shown as top priority. You can then scroll in the list in a more concentrated manner.

? You can use the ***ID*** to uniquely assign actions to individual emails. Hence, transactions with the same ID always belong together (e.g., *12345 Download email*, *12345 Process email*, *12345 Send email*).

Virus results

In the Virus results area, you get detailed information about when *G Data MailSecurity* detected an infected email, which measures were consequently taken, the type of virus, and the actual sender and recipient of this affected email.

You can use the **Virus information** button to call up the ***AntiVirusLab*** website in order to obtain detailed information about the virus discovered. Use **Delete** to remove the selected virus alert from the virus results list.

Administrator menu bar

Here you will find superordinate functions of the administrator software.

Options

In the Options area you can set a vast range of settings to configure *G Data MailSecurity* optimally to the conditions in your network. To do so, you can use various settings areas arranged by topic on various tab pages that you can bring to the front by clicking on the respective tab.

Incoming (SMTP)

In this area you can enter all settings required for scanning incoming ***SMTP email*** for viruses on your mail server.

Received

Here you can specify whether ***Incoming email*** should be processed. In general, ***port 25*** is initialised for this. If this ***standard port*** should not be used under particular circumstances, you can also define other port settings and protocol settings for incoming email via the button **Configure**.

Forwarding

To ***forward*** incoming email to your mail server please disable the **Use DNS to send email** option and specify the desired server under **Forward email to this SMTP server**. Please also specify the **port** via which email is to be forwarded to the SMTP server. If multiple network cards are available, you can specify which of these cards you would like to use in the selection under **Sender IP**.

Protection prior to relaying

To prevent your mail server from being abused, you should specify the domains to which SMTP email may be sent under **Only accept incoming email from the following domains**. This way, your server cannot be misused for forwarding SPAM messages to other domains.

? ***Warning***: If you do not enter any domains here, no emails are accepted either. If all email from all domains are supposed to be accepted, you must enter ***.*** (asterisk dot asterisk) here.

If you want, you can also implement ***relay protection*** using a list of valid email addresses. Email to recipients that are not on the list are not accepted. To automate the maintenance of these email addresses, these can be read automatically and periodically from the ActiveDirectory. The ***ActiveDirectory connection*** requires, as a minimum, ***Net-Framework 1.1***.

? ***ActiveDirectory*** is a database used in Microsoft Windows in which the administrator can centrally organise, deliver and monitor information about objects (e.g., services, resources or users) in the network.

Outgoing (SMTP)

In this area you can enter all settings required for scanning outgoing ***SMTP email*** for viruses on your mail server.

Received

Use the **Process outgoing email** checkmark to specify whether you generally want to check outgoing SMTP email for viruses or not. Under **IP addresses/subnets for computers that send outgoing email** you can specify from which IP addresses the email to be checked originates. If there are several possible IP addresses, please use a comma to separate the individual IP addresses. This input is required so that the email gateway can distinguish between incoming and outgoing email. In general, ***port 25*** is initialised for the receipt of outgoing emails. If this standard port should not be used under particular circumstances, you can also define other port settings and protocol settings for incoming email via the button **Configure**.

Forwarding

Activate the **Use DNS to send email** setting so that emails are sent directly to the mail server that is responsible for the target domains. If you want to send email directly via a ***relay*** (e.g., a provider), disable **Use DNS to send email** and specify the relay under **Forward email to this SMTP server**. If multiple ***network cards*** are available, you can specify which of these cards you would like to use in the selection under **Sender IP**.

Incoming (POP3)

In this area you can enter all the settings required for scanning incoming ***POP3 email*** for viruses on your mail server.

Enquiries

Use **Process POP3 enquiries** to enable the option of using *G Data MailSecurity* to fetch your ***POP3 emails*** from the respective POP3 server, check them for viruses and forward them to their recipients via your email server. Where applicable, you must specify the **port** that uses your email program for POP3 enquiries (normally ***port 110***). Use the **Prevent email program timeout** function to cover the time that *G Data MailSecurity* requires for checking the emails and thus prevent the recipient from getting a ***timeout error*** from the email program when he/she retrieves his/her POP3 emails because the data is not available immediately (depending on the amount of email, there can be a delay of several seconds).

? POP3-based email programs can be ***configured manually***. In doing so, use ***127.0.0.1*** or your email gateway server as the inbound POP3 server in your email program and write the name of the external email server separated from your user name with a colon. Thus, for example, instead of *POP3 server:mail.xxx.de/user name:Jane Q. Public*, you write*POP3 server:127.0.0.1/user name: mail.xxx.co.uk:Jane Q. Public*. To perform a manual configuration, please also refer to the manual of your email program for the steps required for manual configuration.

Collection

Under **Collect email from this POP3 server**, you must specify the POP3 server from which you retrieve email (e.g., *pop3.mailserviceprovider.co.uk*).

Filters

If ***POP3 email*** is rejected based on a content check or due to a virus infection, the sender of this message can be automatically informed of this. The **replacement text for rejected email** is: ***The message was rejected by the system administrator***. However, you can also customise the text for these notification functions. You can also use wildcards here to copy the information relating to the rejected email into the notification text. In the text you define for the Subject and the Email text, the following ***wildcards*** (defined using a percentage symbol followed by a lower case letter) are available:

- %v ***Virus***
- %s ***Sender***
- %r ***Recipient***
- %c ***Cc***
- %d ***Date***
- %u ***Subject***
- %h ***Header***
- %i ***Sender IP***

Virus check

The virus check lets you set virus check options for incoming and outgoing email:

Incoming

Of course, you should normally enable the **Check incoming email for viruses** function and also check which option you want to use **in case of an infection**.

- **Log only**
- **Disinfect (if not possible: log only)**
- **Disinfect (if not possible: rename)**

- **Disinfect (if not possible: delete)**
- **Rename infected attachments**
- **Delete infected attachments**
- **Delete message**

You should only use options in which incoming viruses are merely **logged** if your system is permanently protected from viruses some other way (e.g., using the client/server-based virus protection *G Data AntiVirus*).

If ***a virus is found*** you have a wide range of ***notification options***. You can add a virus alert to the subject and text of the infected email in order to inform the recipient of such an email. You can also send a virus discovery alert to inform certain persons such as system administrators or those employees responsible that a virus has been sent to an email address in your network. Please separate multiple recipient addresses with a semicolon.

You can customise the text for the notification functions. You can also use wildcards here to copy the information relating to the rejected email into the notification text. In the text you define for the **Subject** and **Email text**, the following wildcards (defined using a percentage symbol followed by a lower case letter) are available:

- %v ***Virus***
- %s ***Sender***
- %r ***Recipient***
- %c ***Cc***
- %d ***Date***
- %u ***Subject***
- %h ***Header***
- %i ***Sender IP***

Outgoing

In general you should, of course, enable the **Check outgoing email for viruses** function and have **Do not send infected messages** activated by default. This way, viruses cannot leave your network and therefore cannot possibly cause any damage to your business partners. If a virus is found you have a wide range of ***notification options***. Thus you can choose **Notify sender of infected email** and under **Send virus alert to the following persons** notify, for example, the system administrator or responsible employee of the fact that a virus was about to be sent from your network. Please separate multiple recipient addresses with a semicolon. You can customise the text for the notification functions. To do this, simply click the ••• button on the right. You can also use ***wildcards*** here to copy the information relating to the rejected email into the notification text. In the text you define for the **Subject** and **Email text**, the following wildcards (defined using a percentage symbol followed by a lower case letter) are available:

- %v ***Virus***
- %s ***Sender***
- %r ***Recipient***
- %c ***Cc***
- %d ***Date***
- %u ***Subject***
- %h ***Header***
- %i ***Sender IP***

In addition, under **Attach report to outgoing (uninfected) email**, you have the option of sending email checked by *G Data MailSecurity* with a report at the end of the email text pointing out explicitly that this mail has been checked by *G Data MailSecurity*. But, of course, you can also customise this report or leave it out entirely.

G Data AntiVirus Business

If you have installed the client/server-based virus protection *G Data AntiVirus* (e.g., as part of the *G Data AntiVirus Business or G Data AntiVirus Enterprise solution*), you can set the checkmark for **Report virus results to G Data AntiVirus Business** to make sure that the *G Data AntiVirus* client/server-based antivirus software is informed of MailGateway virus discoveries and thus provides you with a comprehensive overview of virus infections or risks to your network.

Scan parameters

In this area, you can optimise the virus detection performance of *G Data MailSecurity* and configure it to your individual requirements. In general, reducing the virus detection performance increases the performance of the overall system whilst increasing it might result in slight performance losses. This must be considered in each individual case.

The following functions are available:

- **Use engines**: *G Data MailSecurity* uses two antivirus engines; essentially two, independently operating, virus scanner units. Under **Use engines** you can define how these cooperate with each other. In principle, you must use both engines to guarantee optimum virus prevention results. On the other hand, using a single engine improves performance. That is, if you are only using one engine, the analysis operation can be performed more quickly.

- **File types**: Under **File types** you can define the file types *G Data MailSecurity* should check for viruses. Here we recommend automatic type recognition for automatic checking only of files which might theoretically contain a virus. If you want to define the file types to be checked for viruses yourself, use the **user-defined** function. By clicking the ••• button you can open a dialogue box in which you enter the file types you want into the upper input field and then use the **Add** button to add them to the list of user-defined file types. You can also use ***wildcards***, i.e. replace characters or strings of characters with the following symbols:

  The question mark symbol (?) represents individual characters.

  The asterisk symbol (*) represents entire character strings.

? For instance, in order to check all files with the file extension ***.exe***, enter ****.exe***. For example, to check files with different spreadsheet formats (e.g., ***.xlr***, ***.xls***), simply enter ****.xl?***. For instance, to check files of various types that have identical initial file names, enter ***text*.**** for example.

- **Heuristics**: In a heuristic analysis viruses are not only detected using the constantly updated virus databases but also using certain features characteristic of viruses. On the one hand, this method is an additional security benefit; on the other hand, it can also lead to false alarms in rare cases.

- **Check archives**: Checking of ***packed files*** in archives should generally be activated.

- **OutbreakShield**: The OutbreakShield detects and neutralises threats from malicious programs in mass emails before the relevant up-to-date virus signatures become available. OutbreakShield uses the Internet to monitor increased volumes of suspicious email, enabling it to close the window between the mass email outbreak and its containment with specially adapted signatures, almost in real time. If you want to use ***OutbreakShield***, use the **Settings** button to specify whether you are using a proxy server and, if necessary, the **Access data for Internet connection** to enable OutbreakShield to access the Internet at anytime. On the **OutbreakShield** tab, you can define the text of the email that a mail recipient receives if a mass email addressed to him/her has been rejected.

? Due to its independent architecture, OutbreakShield cannot disinfect, rename or quarantine infected email attachments. Hence, the ***replacement text*** informs the user that the suspicious or infected email was not delivered to him/her. There is no alert for email rejected by OutbreakShield, if you select the **Delete message** item on the **Virus check** tab under **In case of an infection**. In this case, all infected emails, including those that have been only detected by OutbreakShield, are deleted directly.

Queue

In this area, you can specify how often and at what intervals resending of email that cannot be forwarded from MailGateway to the corresponding mail server should take place.

Email can be in the queue for a number of reasons. For example, the mail server to which they are to be forwarded after the virus check may be overloaded or may have failed.

? In general, email only reaches the queue after a virus check by *G Data MailSecurity*.

Undeliverable messages

Under **Repeat interval** you can specify at which intervals *G Data MailSecurity* should to start another send attempt. For example, the entry ***1, 1, 1, 4*** means that *G Data MailSecurity* tries to send the email every hour for the first three hours and from then on at regular intervals of 4 hours. Under **Error waiting time** you can specify when the sending of the email is to be terminated permanently and the email is to be deleted.

You can **Notify senders of messages in the queue every x hours** whereby ***x*** must be a full hour value. If you do not wish to inform the sender of an undeliverable message regularly, simply enter a ***0*** here.

? Even if you deactivate the regular notification of senders of non-forwarded email, the sender is, of course, still informed when the delivery of his email has finally failed and the email has been deleted from the server.

You can use the **Reset to default values** button to restore the default settings in the Queue area. These are tried and tested settings.

Size limit

You can limit the size of the queue if you wish. The purpose of this is to protect you from ***Denial of Service attacks***. If the size limit is exceeded, no further emails are added to the queue.

Advanced

In the **Advanced** area, you can change the global settings for *G Data MailSecurity*.

Computer name

If necessary, you can change the computer name (***FQDN*** = ***Full Qualified Domain Name***) of the mail server here.

Limit

To limit the number of SMTP connections that *G Data MailSecurity* processes simultaneously, please set the checkmark for **Limit number of SMTP client connections**. *G Data MailSecurity* then only permits the maximum number of connections that you specify. This way, you can adjust the mail filtering to the performance of the hardware that you are using for the mail gateway.

System messages

The sender address for system messages is the email address that is, for example, used to inform the sender and recipient of virus infected email or to inform them that their emails are in the queue. *G Data MailSecurity system warnings* are independent of the general notifications for virus discoveries. A ***system warning*** usually provides more general, global information, which is not related to an individual, possibly infected email. For example, *G Data MailSecurity* would issue a system warning if virus scanning was no longer guaranteed for any reason. The recipient address(es) for system warnings can, for all intents and purposes, be identical to the addresses that you are using under ***Incoming/outgoing (SMTP, POP3)***.

Settings

You can also save the program option settings as an ***XML file*** using the **Import** and **Export** buttons and thus, if necessary, import again when the need arises.

Change password

This is where you can change the ***administrator password*** that you assigned when you started *G Data MailSecurity* for the first time. Enter the current password under **Old password** and then the new password under **New password** and **Confirm new password**. When you click the **OK** button, the password is changed.

Update

In the update area you can set a vast range of settings to configure *G Data MailSecurity* optimally to the conditions in your network. Here, you can update the virus signatures and program data of *G Data MailSecurity* manually or automatically.

Settings

This is where you can create basic settings for the Internet update. If (e.g., as part of the *G Data AntiVirus Business solution*) you are using the client/server-based *G Data AntiVirus* in parallel with *G Data MailSecurity* you can avoid duplicating the downloads by selecting **Use G Data AntiVirus Client virus signatures** and get them directly from ***G Data AntiVirus***, which will have already saved them on your server. If you choose **Run virus signatures Internet update yourself**, *G Data MailSecurity* performs this operation autonomously. The **Settings and scheduling** button takes you to the area where you can enter all the settings required for manual and automatic updates.

Login data

Under **Login data**, enter the user name and password that you received when you signed up for *G Data MailSecurity*. Click the **Login to server** button if you have not yet logged on to the *G Data Server* yet. The *G Data Server* will use this data to recognize you, and the virus signatures update can be executed completely automatically.

? If you have not ***logged on to the server*** yet, you can do so now. Simply enter the login number (you can find it at the back of the user manual) and your customer data and click **Send**. The login data (user name and password) will be displayed immediately. You should write down this data and keep it in a safe place. Of course, you need an Internet connection to log on to the server (and also for updating virus signatures via the Internet).

Virus update scheduling

The **Virus update scheduling** tab allows you to specify when the automatic update should run and how often. You set up the default schedule under **Run** and then specify in more detail by entering the **Time**.

? Under **Daily** you can use the settings in **Weekdays** to specify, for example, that your computer should only carry out the update on working days or just every other day, or specifically on weekends only when it is not being used for work. To change the time and date under **Time**, simply highlight the item you wish to change (e. g., day, time, month, year) with the mouse and use the arrow keys or the small arrow symbols to the right of the input box to scroll up and down chronologically within the relevant item.

Internet settings

If you use a computer behind a ***firewall***, or if you have other special settings for your Internet access, please use a ***proxy server***. You should change these settings only if your Internet update does not work. If necessary, ask your Internet Service Provider about the proxy address.

The Internet connection login data (user name and password) is especially important if the automatic Internet update is based on a schedule. Without this information, an automatic connection to the Internet cannot be established. Please be sure to enable ***automatic login*** in your general Internet settings (for example, for your mail program or web browser). *G Data MailSecurity* can start the Internet update process without automatic dialling, but it has to wait for you to confirm the Internet connection by selecting **OK**.

User account

Under **User account**, please enter a user account on the MailGateway computer that has access to the Internet.

? ***Warning***: Please do not confuse the entries you make in the **Login data** and **User account** tabs.

Virus signatures

The **Virus update** and **Update status** buttons enable you to start a current virus signature update irrespective of the entries you have made under Scheduling.

Program files

The **Program update** button lets you update the *G Data MailSecurity* program files as soon as changes or improvements have been made.

Spam filter

The spam filter provides you with an extensive range of settings options for effectively blocking email with undesirable content or from undesirable senders (e.g. mass email senders). The program checks for numerous email characteristics that are typical of spam. These characteristics are used to calculate a value reflecting the likelihood of it being spam. To this end multiple tabs are available providing you with all the relevant settings options sorted by subject.

Filters

You can give an individual name to each filter by entering it in the **Name** field, and you can add additional information that may be required in the **Note** field. Under **Reaction** you can define how the spam filter should handle email that may possibly contain spam. You can use the spam probability value calculated for the affected email by ***G Data MailSecurity*** to define three different levels of filtering. How email messages in which ***G Data MailSecurity*** finds individual spam elements are handled is defined under **Suspected spam**. Such messages are not necessarily all ***spam***, but can also be email newsletters or part of a mass emailing that is of interest to the recipient. In such cases, it is recommended that you inform the recipient that the email is suspected spam. **High spam probability** covers emails that contain many spam characteristics and that are rarely of interest to the recipient. **Very high spam probability** collects email that meets all the spam criteria. Such emails are rarely wanted, and rejecting email with these characteristics is recommended in most cases.

? You can improve spam detection by ***forwarding*** such emails to ***G Data***. However, you can also disable this option, of course

Each of these three graduated reactions can be customised.

The **Reject message** option allows you to specify that the email does not even reach your mail server. In this case, the recipient will never receive this email. You can use **Insert spam warning in subject and text of infected email** to inform the email recipient that the email may be spam. You can use the **Notify message sender** option to automatically send a reply to the sender of the email, in which you can notify the sender that his/her mail has been identified as spam. Since many email addresses are only used once for spam, you should think about whether you want to use this function. You can use the **Forward to the following persons** option to forward suspected spam emails, e.g., to the system administrator.

Whitelist

Certain sender addresses or domains can be explicitly excluded from suspected spam via the Whitelist. Simply enter the email address you want (e.g., *newsletter@gdata.de*) or Domain (e.g.*gdata.de*) that you want to exclude from suspected spam in the **Addresses/Domains** field, and *G Data MailSecurity* will not process messages from that sender or sender domain as spam. You can use the **Import** button to insert predefined lists of email addresses or domains into the whitelist. Each address or domain must be listed on a separate line. A plain txt file format is used for storing this list; you can create this list using Windows Notepad for example. You can also use the **Export** button to export whitelists as text files.

Blacklist

Certain sender addresses or domains can be explicitly flagged as suspected spam via the blacklist. Simply enter the email address (e.g., *newsletter@megaspam.de.vu*) or domain (e.g., *megaspam.de.vu*) that you want to mark as suspected spam in the **Addresses/Domains** field, and *G Data MailSecurity* will process messages from that sender and/or sender domain as **emails with very high spam probability**. You can use the **Import** button to insert predefined lists of email addresses or domains into the blacklist. Each address or domain must be listed on a separate line. A plain txt file format is used for storing this list; you can create this list using Windows Notepad for example. With the **Export** button you can export blacklists as text files.

Real-time blacklists

You can find blacklists on the Internet that contain the IP addresses of servers known to send spam. *G Data MailSecurity* uses DNS enquiries to the ***RBLs*** (***real-time blacklists***) to determine whether the sending server is listed. If it is, this increases the probability that it is spam. In general we recommend that you use the default setting here, although you can also add your own Internet addresses for ***blacklists*** under ***blacklist 1, 2 and 3***.

Keywords (subject)

You can also identify suspected spam messages through the words in the ***subject line*** by defining a list of keywords. An occurrence of at least one of the listed terms in the subject line increases the probability of spam. You can change this list as you like by using the **Add**, **Change** and **Delete** buttons. You can add predefined lists of keywords to your list using the **Import** button. Entries in such a list must be listed one below the other in separate lines. A plain txt file format is used for storing this list; you can create this list using Windows Notepad for example. You can also use the **Export** button to export such a list of keywords as a text file. By selecting the **Find whole words only** option, you can have *G Data MailSecurity* search the email text for whole words only. So if *cash* has been defined as a keyword, messages containing that word would be suspected as spam, while messages containing *cashew nuts* in the text would not be affected.

Keywords (email text)

By defining a list of keywords you can also identify suspected spam through the words used in the ***email text***. If at least one of these terms is included in the email text, the spam probability increases. You can change this list as you like by using the **Add**, **Change**, and **Delete** buttons.

You can add predefined lists of keywords to your list using the **Import** button. Entries in such a list must be listed one below the other in separate lines. A plain txt file format is used for storing this list; you can create this list using Windows Notepad for example. You can also use the **Export** button to export such a list of keywords as a text file. By selecting the **Find whole words only** option, you can have *G Data MailSecurity* search the email text for whole words only. So if *cash* has been defined as a keyword, messages containing that word would be suspected as spam, while messages containing *cashew nuts* in the text would not be affected.

Content filter

The content filter has been designed as a self-learning filter based on the Bayes method, and it calculates spam probability on the basis of the words that are used in the text of the message. This filter not only works on the basis of predefined word lists but also learns from each new email received. You can view the word lists that are used by the content filter for identifying email as spam via the **Query table contents** button. You can delete all learned table content by using the **Reset tables** button, after which the content filter will restart its learning process again from the beginning.

Advanced settings

In this area, you can make very detailed changes to the *G Data MailSecurity* spam detection and configure it to the mail server environment. However, we generally recommend using the default settings here. Making changes in the advanced settings should only be done if you have the corresponding expertise and know exactly what you are doing.

Attachment

Troubleshooting (FAQ)

In this area you can find answers to questions which may arise while you are working with *G Data MailSecurity*.

- **I am using AVM Ken! and want to install G Data MailSecurity on the same computer as the Ken! server**: For detailed instructions, please contact our ***support team***.
- ***I am using an Exchange Server 2000 and want to install G Data MailSecurity on the same computer as the Exchange Server. How can I change the ports for incoming and outgoing email in Exchange Server?*** For detailed instructions, please contact our ***support team***.

Notes

Index

K

L

M

N

O

T

U

V

W

X