

G DATA

# Security Software



# Table of Contents

<b>First steps</b>	<b>4</b>
+ ServiceCenter	
+ Installation	
<b>SecurityCenter</b>	<b>7</b>
+ Status displays	
+ License	
+ Software modules	
<b>Virus protection</b>	<b>12</b>
+ Virus check	
+ Quarantined files	
+ Boot medium	
<b>Firewall</b>	<b>14</b>
+ Status	
+ Networks	
+ Rule sets	
<b>Backup</b>	<b>18</b>
+ Backup and restore	
<b>Password Manager</b>	<b>23</b>
+ Using the browser plug-in	
<b>Tuner</b>	<b>25</b>
+ Restore	
+ Browser Cleaner	
<b>Parental controls</b>	<b>27</b>
+ Create new user	
+ Forbidden content	
+ Permitted content	
+ Monitor Internet usage time	
+ Monitor computer usage period	
+ Personal filters	
+ Settings: Log	
<b>Encryption</b>	<b>30</b>
+ Create new safe	
+ Create mobile safe	
+ Open mobile safe	
<b>Autostart Manager</b>	<b>33</b>
+ Properties	
<b>Device control</b>	<b>34</b>

<b>Settings</b>	<b>35</b>
+ General	
+ AntiVirus	
+ AntiSpam	
+ Firewall	
+ Tuner	
+ Device control	
+ Backup	
<b>Logs</b>	<b>53</b>
+ Virus protection logs	
+ Firewall logs	
+ Backup logs	
+ Spam protection logs	
+ Parental controls logs	
+ Device control logs	
<b>FAQ: boot scan</b>	<b>54</b>
<b>FAQ: Program functions</b>	<b>56</b>
+ Security icon	
+ Run virus check	
+ Virus alarm	
+ Firewall alarm	
+ Not a virus message	
+ Uninstall	
<b>FAQ: License questions</b>	<b>60</b>
+ Multi-user licenses	
+ Licence renewal	
+ Changing computers	
+ Copyright	

# First steps

We are delighted that you have chosen our product and hope that you are entirely satisfied with your new G DATA software. If something does not seem to work straight away, our help documentation will be of assistance to you. If you have any other questions, our experts in the **ServiceCenter** are at your disposal.

**Note:** You can consult the comprehensive help pages within the software at any time to get all the information you need straight away. To do so, just click the help icon displayed in the software.

## ServiceCenter

Installation and use of G DATA software is easy and self-explanatory. However, if you encounter a problem, just get in touch with our competent support representatives in our ServiceCenter:

G DATA United Kingdom      [www.gdatasoftware.co.uk](http://www.gdatasoftware.co.uk)

G DATA USA      [www.gdata-software.com](http://www.gdata-software.com)

G DATA International      [www.gdatasoftware.com](http://www.gdatasoftware.com)

## Installation

If your computer is or has already been protected by antivirus software, you can run the installation as follows. If you are still reasonably sure that your computer is infected with a virus, you are recommended to run a **BootScan** prior to installing the software.

**Warning:** If you were previously using antivirus software from another vendor, this should be completely uninstalled from your computer beforehand. As antivirus software integrates deeply within the Windows operating system, it is recommended that you not only run the normal uninstall for the software but – if possible – also use the cleaning tools that the vendor provides via their online support center.

### Step 1 - Starting the installation

Launch the installation as follows:

- **CD/DVD installation:** To begin the installation, place the software CD or DVD in the tray.
- **Software download:** Just click on the downloaded file to begin installing a version of the software downloaded from the Internet.

An installation window will open automatically.

**Note:** If the installation does not start: It may be that you have not set up the autostart function on your computer. The software cannot then start the installation process when the software CD is inserted and the window you use to install the G DATA software does not open.

- If an autoplay selection window opens instead, click on the **Run AUTOSTRT.EXE** option.
- If the option window does not open, please use Windows Explorer to search for the data medium with the G DATA software on it and then run the **Setup** or **Setup.exe** file.

### Step 2 - Selecting the language

Please select the language your new G DATA software should be in when you install it.

### Step 3 - Installation methods

A wizard then guides you through the process of installing the software on your computer. Now select whether you want to run the default installation or a user-defined installation. We recommend the default installation.

**Malware Information Initiative:** G DATA SecurityLabs is constantly investigating ways of protecting G DATA customers against malware (viruses, worms, and malicious software). The more information there is available, the more effectively the protection mechanisms can be developed. There is plenty of information available, but only on systems that are attacked or infected. The G DATA Malware Information Initiative was founded to enable such information to be included in the analysis. Malware-related information is sent to G DATA SecurityLabs in this context. Through your participation, you are contributing to helping all G DATA customers make the Internet safer to use. When installing the G DATA software, you can decide whether you want to send information to G DATA SecurityLabs or not.

**Note:** With the user-defined installation, you can select the storage location you want for the program data and enable or disable software modules (e.g. spam protection) during the installation.

## Step 4 - License agreement

Now read the license agreement and agree to it.

## Step 5 - User-defined installation (optional)

If you have selected user-defined installation, two wizard windows now appear in which you can specify the installation directory for the software and the range of modules to install. If you have selected the default installation, you can skip this step.

- **User-defined:** Here you can specify the scope of the installation by checking the checkboxes for the various software modules (e.g. AntiSpam etc.).
- **Complete:** All the modules in your version of the software will be installed.
- **Minimal:** With the AntiVirus module, only the basic virus protection in your G DATA software is installed.

**Updates:** You can use setup to install software modules or update your software at any point in the future. Simply restart the setup and select **Customize Installation** to increase or reduce the software modules. If you have a new software version and want to update it, you can specify which additional modules to select/deselect under the **User-defined Update** option.

## Step 6 - Software version

Here you can also specify whether you want to install the software as a full version or as a trial version. If you have purchased the software and have a registration number, you should of course select the **Full version** option. To help familiarize yourself with the G DATA software for free, you can simply take advantage of our time-limited trial access.

## Step 7 - Product activation

Product activation occurs during installation. Here you can activate your software.

- **Enter a new registration number:** If you reinstall your G DATA software, please select this option and enter the registration number that came with the product. Depending on the type of product, you will find this, for example, on the back of user manual, in the confirmation email for a software download or on the product packaging.

**Note:** The product will be activated on entering the registration number. You will also receive an email with your access data for subsequent use.

- **Enter access data:** If you have already activated your G DATA software, you will have received your access data (user name and password). After reinstalling the software or to register another computer (with a multi-user license), just enter the access data here.

**Note:** You will only receive the access data via email. No access data is delivered with the product itself.

If you have lost or forgotten your access data, go to the login page and click on the **Access data misplaced?** entry. A website opens where you can enter your registration number. When you have done so, your access data will be re-sent to the email address you entered during registration. If your email address has changed in the mean time, please contact our **ServiceCenter**.

- **Activate later:** If you just want to evaluate the software, you can also install it without entering any data. However, if you do so, no Internet updates can be downloaded by the software, and you will not have adequate protection against malware. You can enter your registration number or access data subsequently at any time by performing an update.

## Step 8 - Finishing the installation

You may have to restart your computer after the installation is complete. Your G DATA software is then available.

## After the installation

After installing you can launch your newly installed G DATA software via the software icon in the taskbar. Furthermore there are now additional security functions available on your computer:



**Security icon:** Your G DATA software permanently protects your computer against malware and attacks. An icon in the computer's taskbar tells you as soon as the software considers intervention by the user to be necessary. You can open the G DATA program interface by right-clicking the icon. Please read about this in the section entitled [Security icon](#).



**Shredder:** If you have selected the shredder during installation (not integrated with G DATA Antivirus), this is available as a desktop icon. Data you move to the shredder will be removed in such a way that it cannot be restored, even using professional data recovery tools. In doing so the data is overwritten using a fully customizable number of processes. You can access the settings by right-clicking the shredder icon and calling up the properties.





**Fast check:** The fast check enables you to easily check files without having to launch the software at all. Just use the mouse to highlight files or folders in Windows Explorer, for example. Now right-click and select **Check for viruses** in the dialog window that appears. The affected files will now be automatically scanned for viruses.

**Your computer starts differently than usual after installing the software:** This may be because the software CD is still in the drive. Simply remove the CD and your computer will restart as normal.

# SecurityCenter

You only need to consult the SecurityCenter if you want to access one of the software's many additional features. The actual protection of your computer against viruses and other threats takes place all the time in the background. In cases where the software requires your intervention, you are automatically reminded of this via information in your computer's taskbar.




## Security status

-  As long as there is a green checkmark everywhere, your system is protected.
-  A red exclamation mark indicates that your system is in immediate danger. You should then undertake immediate measures so that the protection of your data remains ensured.
-  If the placeholder icon is shown, this means that the relevant security function has not been activated by you (e.g. spam protection).
-  A yellow icon indicates that the user will soon need to intervene. This is the case, for example, if there is a program update for the software.

You can then use all the other software functions and program areas (e.g. **virus protection** or **settings**) if you prefer to actively look after the security of your system yourself - but you mustn't! You decide to what degree you would like to be involved with the subject of virus protection and data security. The product provides you with extensive online help.

## Global functions

The following icons indicate the security status of the respective area.

-  **Settings:** You can use this button at the top right to access all settings dialogs for the various areas of the software. You also have the option of directly selecting the appropriate settings dialogue in each area.
-  **Logs:** Here the software lists the current logs on all actions carried out (virus checks, updates, virus discoveries, etc).
-  At the upper right in the header line of the software you can also find the following functions:
  - Show help:** You can consult the executable help software in the program at any time. To do so, just press the help button displayed there in the software.
  - Update software:** When new program versions of the software are available, you can easily update these with one click, as with the virus information. Should you receive information here that an update is available, simply click on the Update Program option. Detailed information can be found in the section: [Updates](#)
  - About:** This is where you get information about the program version. The version number can be helpful, for example, when talking to the [ServiceCenter](#).

## Status displays

The following status displays tell you about the security status of your system. If you click on these entries, you can immediately carry out actions to optimize the security status:

### Real-time protection

The virus monitor real-time protection continuously checks your computer for viruses; it controls read and write operations, and as soon as a program attempts to execute malware or spread malicious files it prevents it from doing so. The virus monitor is your most important protection! It should never be switched off.

- **Disable virus monitor:** However, if you need to switch off the virus monitor, you can do so here. If you want to optimize the performance of your computer by switching off the monitor, please ensure that you check whether you can achieve the desired result using another virus monitor setting. For this purpose, when you switch off the virus monitor you have the option of accessing the relevant settings changes. To do this, click simply on [Change security/performance](#) and follow the instructions in the help section with the same name. Alternatively you can of course switch the virus monitor off completely as well.
- **Disable behavior monitoring:** Behavior monitoring involves intelligent detection of unknown malware, offering additional

protection independently of virus signatures. Behavior monitoring should generally be enabled.

- **More settings:** You can find more information on this in the section [Settings | AntiVirus | Real-time protection](#).

## Last idle scan

This is where you can see when your computer was last fully checked for viruses. If this entry is highlighted in red, you should run a virus check as soon as possible.

- **Check computer:** If you have time and do not need to use the computer for work for the next few hours, you can launch a full scan of the computer directly from here. You can continue using the computer during this time. However, as the virus check is running at maximum performance with this setting, it may take longer for other applications to respond. For further information, see the section [Virus check](#).
- **Run idle scan now:** The idle scan will launch automatically during periods in which your computer is inactive. In this way it will run a check on the entire computer at automatically determined intervals. If you want to launch the idle scan before the next automatically determined date, please select **Start idle scan now**. If you do not want the G DATA software to automatically launch the idle scan during breaks in work, you can also disable this function under **Disable idle scan** (not recommended).

## Firewall

A firewall protects your computer from being *spied on*. It checks which data and programs from the Internet or network reach your computer and which data is sent from your computer. As soon as there is an indication that data is to be installed or downloaded on your computer without authorisation, the firewall alarm sounds and blocks the unauthorised data exchange. This software module is available in the G DATA Internet Security and G DATA Total Security software versions.

- **Disable firewall:** You can disable the firewall completely if required. This means that your computer is still connected to the Internet and any other networks, but the firewall is no longer protecting it against attacks or electronic espionage (not recommended).
- **Disable autopilot:** It is generally advisable to use the firewall in **autopilot** mode. It then virtually runs in the background and protects you without you having to undertake major settings. If you are using the firewall without the autopilot, a dialog will appear in the event of doubt in which you can gradually optimize the firewall for your system environment. This is a helpful feature for experienced users. Disabling the autopilot is not normally recommended.
- **More settings:** You can find more information on this in the section [Settings | Firewall | Automatic](#).

## Web protection

In this area you can enable/disable web protection. Web protection is a module that automatically detects threats when surfing the Internet or downloading files and renders them harmless if necessary. This is a useful aid to the virus monitor and blocks harmful websites and downloads before they can even be accessed.

If a website is identified as a threat by the G DATA software and blocked, you will see an information page from G DATA displayed in the browser instead of the website.

- **Disable web protection:** If you disable web protection, this can create a time benefit with, for example, very large downloads from a secure source. Generally your computer is still protected by the virus monitor when web protection is disabled. Nevertheless you should only prevent web protection in exceptional cases.
- **Define exceptions:** Web protection ensures that you do not fall victim to infected or fraudulent websites on the Internet. However, in rare cases it may occur that a website is not displayed properly, even though it is supplied by a safe provider. In such a case, you can add this web address to the Whitelist, i.e. you can define it as an exception and Web protection will no longer block this site. You can read the section entitled [Define exceptions](#) to find out how to do this.
- **More settings:** You can find more information on this in the section [Settings | AntiVirus | Web protection](#).

## Email check

The email check enables you to scan incoming and outgoing emails and file attachments for viruses and eliminate possible infections at the source. The software can directly delete file attachments or repair infected files if viruses are found.

- **Disable email protection:** Please select this option if you do not want the G DATA software to check emails. However, disabling this entails a high security risk and should only be done in exceptional cases.
- **More settings:** You can find more information on this in the section [Settings | AntiVirus | Email check](#).



**Microsoft Outlook:** Here emails are scanned by a plugin. This provides the same level of protection as the protection function for POP3/IMAP offered by AntiVirus. After installing this plugin, you will find the **Scan folder for viruses** function in the Extras Outlook menu. You can use this to check your email folders individually for virus contamination.

## Spam protection

Special offers, advertising, newsletters – the flood of unsolicited email is ever-increasing. Is your inbox overflowing with vast amounts of unwanted electronic mail? The G DATA software will use a combination of the most up-to-date spam checking criteria to securely protect you from spam/junk mail, block spam senders effectively and prevent false detections. This software module is available in the G DATA Internet Security and G DATA Total Security software versions.

- **Protocol: Spam:** Here you are provided with a comprehensive overview of all emails categorized as spam by the G DATA software. You can use the **Update** button to retrieve the most up-to-date data version for the software and the **Delete** button to delete all previously marked entries. The email messages themselves, which are held in your email client, are not deleted of course. You can use the **Add to whitelist** button to add a highlighted email to the whitelist, thus generally excluding the relevant email address from further spam checks. You can use the **Add to blacklist** button to add a highlighted email to the blacklist, thus generally subjecting the relevant email address to extensive checks for spam elements.
- **Protocol: No spam:** Here you are provided with a comprehensive overview of all emails not categorized as spam by the G DATA software. You can use the **Update** button to retrieve the most up-to-date data version for the software and the **Delete** button to delete all previously marked entries. The email messages themselves, which are held in your email client, are not deleted of course. You can use the **Add to whitelist** button to add a highlighted email to the whitelist, thus generally excluding the relevant email address from further spam checks. You can use the **Add to blacklist** button to add a highlighted email to the blacklist, thus generally subjecting the relevant email address to extensive checks for spam elements.
- **Edit whitelist:** Certain sender addresses or domains can be explicitly excluded from suspected spam via the whitelist. Simply click on the **New** button and enter the email address (e.g. newsletter@infosite.com) or domain (e.g. infosite.com) that you want to exclude from suspected spam in the **Sender addresses/sender domains** field. The G DATA software will treat emails from that sender or sender domain as not 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.
- **Edit blacklist:** Certain sender addresses or domains can be explicitly flagged as suspected spam via the blacklist. Simply click on the **New** button and enter the email address (e.g. newsletter@megaspam.de.vu) or domain (e.g. megaspam.de.vu) that you want to include as suspected spam in the **Sender addresses/sender domains** field. The G DATA software will treat emails from that sender or sender domain as having a 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.
- **Disable spam protection:** If necessary you can disable spam protection on your computer here, e.g. if do not have an email client of any kind installed on your computer.
- **More settings:** You can find more information on this in the section [Settings | AntiSpam | Spam filter](#).

## Last update

This is where you can see when your computer last received updated virus signatures from the Internet. If this entry is highlighted in red, you should run a virus update as soon as possible. To do so just click on the entry and select the **Update virus signatures** option.

- **Update virus signatures:** Normally updates for virus signatures are run automatically. If you want to run an update straight away, please click on this button.
- **Disable automatic updates:** Select this option if you do not want the G DATA software to bother automatically updating the virus signatures. However, disabling this entails a high security risk and should only be done in exceptional cases.
- **More settings:** You can find more information on this in the section [Settings | AntiVirus | Updates](#).

## Next update

Under this entry you can see when the next update will be carried out. If you want to run an update, just click on the entry and select the **Update virus signatures** option.

- **Update virus signatures:** Normally updates for virus signatures are run automatically. If you want to run an update straight away, please click on this button.

- **Disable automatic updates:** Select this option if you do not want the G DATA software to bother automatically updating the virus signatures. However, disabling this entails a high security risk and should only be done in exceptional cases.
- **More settings:** You can find more information on this in the section [Settings | AntiVirus | Updates](#).

## BankGuard

Banking Trojans are becoming more and more of a threat. Every hour, online criminals are developing new malware variants (like Zeus or SpyEye) that they use to steal your money. Banks secure data traffic on the Internet. However, the data is decrypted in the browser and banking Trojans can attack it there. However, the pioneering BankGuard technology from G DATA secures your banking transactions from the outset and provides instant protection where the attack takes place. By checking that the network libraries used are genuine, G DATA BankGuard ensures that your web browser has not been manipulated by a banking Trojan. We recommend leaving G DATA BankGuard protection switched on.

## Keylogger protection

Keylogger protection also monitors whether keyboard input on your system is being spied on, independently of virus signatures. This would give attackers the option of logging your password input. This function should always be enabled.

## Exploit protection

An "exploit" exploits vulnerabilities in popular software and can use them to take control of your computer in the worst case. Exploits can even come into effect when applications (e.g. PDF viewer, browser etc) are routinely updated. Exploit Protection protects you against such access – and proactively protects you against previously unknown attacks.

## License

Under the **License** entry on the left-hand side of the program interface you can see how long your virus update license is valid for. Constant updates are more important for antivirus software than for any other type of software. Therefore the software will automatically remind you to renew your license before it expires. The best way is via the Internet – convenient and easy.

## Login credentials

If you click on **Login credentials** in the License area, a dialogue box appears in which you can view your login credentials. More information can be found in the section [Settings | AntiVirus | Updates](#). If you have any questions regarding your license, the [G DATA ServiceCenter](#) can provide specific help with this information. If you have forgotten your password, you can generate a new password quickly and easily via this dialogue box.

## Protect more PCs / Enhance range of functions

Naturally you can increase the number of licenses you have or upgrade to products with increased functionality at any time. If you click on the **Protect more PCs** entry in the SecurityCenter, you will be taken directly to the online shop on our website. You can use the **Upgrade to get more functions** entry to go to the UpgradeCenter, where you can order the enhanced functionality in our other software versions (subject to special conditions).

## What happens on license expiration?

A few days before your license expires, an information window appears in the task bar. If you click this, a dialogue window opens in which you can extend your license easily in a few steps. Just click on the **Buy now** button, complete your data and your virus protection will be guaranteed again immediately. You will receive the invoice in the next few days via email as a PDF.

**Note:** This dialog only appears at the end of the first year. Thereafter your license will be automatically extended every year. You can cancel this extension service at any time without giving reasons.

## Software modules

The following software modules are available (depending on the software version installed):



**SecurityCenter:** Your personal security center. Here you can find all the information you need to protect your computer against malware, enabling you to respond specifically to threats.



**Virus protection:** In this area you can find information on when your computer was last checked for virus infections and whether the virus monitor is currently providing active protection against infections. Furthermore you can also check the computer or data

medium directly for malware, process infected files in the quarantine folder and create a boot medium.



**Firewall:** A firewall protects your computer from being spied on. It checks which data and programs from the Internet or network reach your computer and which data is sent from your computer. As soon as there is an indication that data is to be installed or downloaded on your computer without authorisation, the firewall alarm sounds and blocks the unauthorised data exchange. This software module is available in the G DATA Internet Security and G DATA Total Security software versions.



**Backup:** As everyday life becomes increasingly digitized through the use of online music services, digital cameras and email, backing up your personal data becomes ever more important. In case there is a hardware error, an accident or damage from viruses or hacker attacks, you should take care to regularly backup your personal documents. The backup module takes care of this job for you and protects your most important documents and files so that you don't have to worry about them. This software module is available in the G DATA Total Security software version.



**Password Manager:** You can use the Password Manager as a handy plug-in for your browser to easily manage passwords. This software module is available in the G DATA Total Security software version.



**Tuner:** From automatic reminders about Windows updates and regular, scheduled defragmentation to regular removal of unnecessary registry entries and temporary files, the tuner is a handy tool for making your Windows system much faster and more manageable. This software module is available in the G DATA Total Security software version.



**Parental controls:** You can use parental controls to regulate surfing behavior and computer use for your children. This software module is available in the G DATA Internet Security and G DATA Total Security software versions.



**Encryption:** The encryption module acts like a safe for protecting sensitive data. A safe can, for example, be used as an extra drive like an additional hard disk partition and is very easy to work with. This software module is available in the G DATA Total Security software version.



**Autostart Manager:** The Autostart Manager enables you to manage programs that are automatically started when Windows starts. Normally such programs are loaded on system start-up. However, when they are managed by the Autostart Manager, they can also be started with a delay or according to the workload of the system or hard disk. This makes system start-up faster and so improves the performance of your computer.



**Device control:** You can use this function to restrict the use of devices such as removable data media, CD/DVD and disk drives for specific users of your computer. In this way for example you can prevent unauthorized importing or exporting of data or software installations. Now also with USB KeyboardGuard. There is more information on this in the Device control section.

# Virus protection

With this module you can scan your computer or selected data medium for malware infections in a targeted manner. This is recommended if, for example, you are given USB sticks from friends, relatives or work colleagues, or you use CDs they have burned. A virus check is also recommended when installing new software or downloading from the Internet.

**Warning:** Scanning the computer or selected data medium acts as additional protection. Basically, with the G DATA idle scan and the G DATA virus monitor, which is constantly working in the background, you have optimum protection against malware threats. A virus check would also detect viruses that were copied onto your computer before you installed the G DATA software or that you picked up while the virus monitor was disabled.

## Virus check

Select which area of your computer or which data medium you want to specifically check:



**Check computer (all local drives):** If you want to check your computer independently of the automatic idle scan (e.g. because you currently have a suspected virus), just click on this entry. Your computer will now be checked for viruses. You can also read about this in the following section: [Run virus check](#)



**Scheduled virus checks:** This function enables you to plan automatic virus checks. You can also read about this in the following section: [Automatic virus checks](#).



**Check memory and Startup:** Here the program files and DLLs (program libraries) for all running processes will be checked. In this way malware can be directly removed from the memory and autostart area. Active viruses can be directly removed without searching through the entire hard drive. However, this function is not a replacement for regular virus checks of saved data, but rather an extension to it.



**Check directories/files:** This enables you to scan selected drives, directories or files for viruses. If you click on this action, a directory and file selection dialog will open. You can scan specific individual files or entire directories for viruses here. In the directory tree, you can open and select directories by clicking the "plus" symbols. Their contents will then be shown in the file view. Each directory or file that you mark with a check will be scanned by the software.

If not all files in a directory are checked, this directory is marked with a gray checkmark.



**Check removable media:** Use this function to check CD-ROMs or DVD-ROMs, memory cards or USB sticks for viruses. If you click on this option, all removable media connected to your computer will be checked (including CDs in the tray, inserted memory cards, hard drives connected via USB or USB sticks). Please note that the software cannot of course remove viruses from media that do not have write access (e.g. burned CD-ROMs). In this case, virus discoveries are logged.



**Check for rootkits:** Rootkits attempt to evade conventional virus detection methods. You can use this function to specifically search for rootkit viruses, without checking all the hard drives and saved data.

## Quarantined files

During the virus check, you have different options for dealing with any viruses found. One option is to move the infected file to quarantine. Quarantine is a secure area in the software where infected files are encrypted and stored so they cannot transfer the virus to any other files.



**Show quarantine:** If you click on this button, the quarantine area opens.

The files in quarantine remain in the condition they were in when the G DATA software found them, and you can decide how to proceed.

- **Update:** If you have kept the quarantine dialogue window open for a long time, and have since discovered a virus and moved it into quarantine (e.g. automatically via the virus monitor), you can use this button to update the view.
- **Allow from now on:** If the behavior monitor has quarantined a file by accident, you can add it to the whitelist to prevent the behavior monitor from moving it to the quarantine in the future.
- **Disinfect:** In many cases, infected files can still be recovered. The software removes the virus components from the infected file and reconstructs the uninfected original file. If the disinfection is successful, the file is moved back to where it was saved before the virus check and is available to you again without any restrictions.

- **Move back:** Sometimes it is necessary to move an infected file that cannot be cleaned back out of quarantine to its original storage location. This may be for data recovery purposes for example. You should only select this function in exceptional cases and observe strict security measures (e.g. disconnect the computer from the network/Internet, back up uninfected data first etc).
- **Delete:** If you no longer require the infected file, you can simply delete it from quarantine.

## Boot medium

The boot medium is a useful tool for ridding your computer of viruses that have already contaminated it. Use of a boot medium is particularly recommended for computers that had no virus protection prior to installing the G DATA software. You can read up on how to use a **boot medium** in the section entitled [boot scan](#).



To create a boot medium, just click on the **Create boot medium** button and follow the installation wizard's instructions. Here you have the option of downloading current virus signatures to bring your boot medium fully up to date. You also have the option of burning a CD/DVD as a boot medium or using a USB stick as a boot medium.

If you are using the G DATA Total Security software version, you can also use a boot medium to restore a drive backup to the volume on which the system is currently located. It is also possible to restore a drive or file backup to another target here. To do so, insert the boot medium and select **Start Restore**.

# Firewall

A firewall protects your computer from being *spied on*. It checks which data and programs from the Internet or network reach your computer and which data is sent from your computer.

There are three areas in the firewall module:

- **Status:** In the Status area of the firewall, you will find basic information about the current status of your system and the firewall.
- **Networks:** The Networks area lists the networks (e.g. LAN, data transmission network etc.) to which your computer is connected.
- **Rule sets:** In this area you can create specific rules for different networks and so optimize the performance of your firewall.

As soon as there is an indication that data is to be installed or downloaded on your computer without authorization, the firewall alarm sounds and blocks the unauthorized data exchange.



**Settings:** You can use this button at the top right to access all the other settings dialogs for the firewall.

## Status

In the status area of the firewall, you will find basic information about the current status of your system and the firewall. You will find this to the right of the relevant entry as either text or numerical data. In addition, the status of components is also displayed graphically. By double-clicking the respective entry, you can carry out actions here directly or switch to the respective program area.

As soon as you have optimised the settings for a component with a warning icon, the icon in the Status area will revert to the green check icon.

- **Security:** As you use the computer for your daily tasks, the firewall gradually learns which programs you do or do not use for Internet access and which programs represent a security risk. Depending on how familiar you are with firewall technology, you can configure the firewall to provide either highly effective basic protection without an excessive number of inquiries or professional protection customised to your own computer usage habits – however this also requires detailed knowledge of firewalls. You can set the security status here: [Settings | Firewall | Automatic](#).
- **Mode:** Here you are informed with which basic setting your firewall is currently being operated. Either manual rule creation or automatic (autopilot) are possible here.

**Autopilot:** Here the firewall works fully autonomously and automatically keeps threats from the local PC. This setting offers practical all-around protection and is recommended in most cases. The autopilot should be switched on by default.

**More settings:** If you would like to individually configure your firewall or do not want particular applications to work together with autopilot mode, you can adjust your firewall protection entirely to your requirements via the manual rule creation. Further information is available in the following section: [Settings | Firewall | Automatic](#).

- **Networks:** Here you can see the networks your computer is part of. You can find more information in the following section: [Firewall | Networks](#).
- **Prevented attacks:** As soon as the firewall registers an attack on your computer, this is prevented and logged here. More information is available by clicking on the menu item.
- **Application radar:** This dialog box shows you which programs are currently being blocked by the firewall. If you still want to allow one of the blocked applications to use the network, simply select it and then click the **Allow** button.

## Networks

The Networks area lists the networks (e.g. LAN, data transmission network etc.) to which your computer is connected. Also shown here is which rule set (see section entitled [Rule sets](#)) are protecting the respective network. If you uncheck the relevant network it will no longer be protected by the firewall. However, you should only disable this protection in specially justified circumstances. If you use the mouse to highlight a network and click on the **Edit** button, you can view and/or change the firewall settings for this network.

## Edit network

The following information and settings options for the selected network will be displayed in this overview:

- **About network:** This is where you can find information about the network, such as – where available – the IP address, subnet mask, default gateway, DNS and WINS server.
- **Firewall enabled on this network:** You can use this option to disable the firewall's network protection, but you should only do this in specially justified circumstances.
- **Internet connection sharing:** If your system connects directly to the Internet, you can specify whether all computers on the network should have access to the Internet via a computer connected to the Internet or not. This Internet connection sharing (ICS) can usually be enabled for a home network.
- **Enable automatic configuration (DHCP):** When you connect your computer to a network, a dynamic IP address is assigned (via DHCP = Dynamic Host Configuration Protocol). You should leave this option checked if you are connected to the network using this default configuration.
- **Rule set:** You can very quickly choose from predefined rule sets and determine whether, in terms of firewall monitoring, you are dealing with a network which can be e.g. trusted, not trusted, or should be blocked. Clicking the **Edit rule set** button gives you the option of configuring rule sets individually. Please also refer to the section [Create rule sets](#).

## Rule sets

In this area you can create special rules for different networks. These rules can then be grouped together to form a rule set. There are default rule sets for direct Internet connection, for untrusted networks, trusted networks, and blocked networks. The relevant rule set is displayed with name in the overview. You can change existing rule sets or add new ones using the **New**, **Delete**, and **Edit** buttons.

The default rule sets for **Direct Internet connection**, **Trustworthy networks**, **Untrustworthy networks**, and **Networks to be blocked** cannot be deleted. You may, of course, delete additional rule sets that you yourself have created at any time.

## Create rule sets

You can allocate every network its own rule set (i.e. a collection of rules specially matched to it). In this manner you can protect networks with different levels of danger in different ways using the firewall. For example, a home network may require considerably less protection (and consequently less administrative effort) than a data transmission network directly connected to the Internet.

Furthermore, you can also create individual rule sets for networks by clicking the **New** button. To do this, click the **New** button in the Rule sets area and enter the following details in the dialog window:

- **Rule set name:** Enter a meaningful name for the rule set here.
- **Generate an empty rule set:** This allows you to generate an empty rule set and enter custom-defined rules.
- **Generate a rule set which contains a number of meaningful rules:** This option allows you to specify if you want the new rule set to include a few default rules for untrusted, trusted or blocked networks. You can then make individual adjustments based on these defaults.

The firewall contains default rule sets for the following network types:

- **Direct Internet connection:** This covers rules that involve direct Internet access.
- **Untrusted networks:** This generally covers open networks (e.g. data transmission networks) with Internet access.
- **Trusted networks:** Home and company networks are generally trusted.
- **Blocked networks:** This setting can be used if the computer's access to a network is to be blocked on a temporary or permanent basis. This is advisable, for instance, when you are connected to unfamiliar networks with an indeterminate level of security (e.g. LAN parties, external corporate networks, public workspaces for laptops, etc.)

The new rule set now appears in the list in the Rule sets area under the relevant rule set name (e.g. *New rule set*). If you then click on **Edit** - depending on the setting you made under [Settings | Other](#) (see the section with the same name) - the Rule wizard or the advanced editing mode for editing the individual rules of this rule set will open. You can learn how to assign new rules in the rule sets in the sections entitled [Using the Rule wizard](#) and [Using the advanced editing mode](#).

In addition to directly entering rules yourself, you can also create rules via the firewall alarm info box. This learning process of the firewall

is explained in the section entitled [Firewall alarm](#).

## Using the Rule wizard

The rule wizard allows you to define specific additional rules for the relevant rule set, or to modify existing rules. We recommend that users unfamiliar with firewall technology use the rule wizard rather than the advanced editing mode.

You can use the rule wizard to change one or more rules in the selected rule set. Thus you always create a rule within a rule set that contains various rules.

Depending on which rule set you have specified for the relevant network, one rule set (e.g. for untrustworthy networks) may block an application while another (e.g. for trustworthy networks) could grant it full network access. This means you can use a strategic combination of rules to restrict a browser in such a way that, for example, it can access websites available within your home network but cannot access content from the data transmission network.

The following basic rules are available in the rule wizard:

- **Allow or block applications:** This allows you to select a specific application (program) on your hard disk and explicitly permit or deny it access to the network governed by the rule set. Simply use the wizard to select the required program (**program path**) then, under **Direction**, indicate whether the program is to be blocked for inbound connections, outbound connections or both inbound and outbound connections. This enables you, for example, to prevent your MP3 player software forwarding data about your listening habits (outbound connections) or to ensure that program updates are not downloaded automatically (inbound connections).
- **Allow or block network services:** A **Port** is a specific address area that automatically forwards data transferred over a network to a specified protocol and then on to specified software. For example, standard websites are transferred via port 80, while email is sent via port 25 and received via port 110, etc. Without a firewall, all ports on your computer normally remain open, although the majority of users do not need most of these. Blocking one or more of these ports is a quick way of eliminating vulnerabilities that could be used for attacks by hackers. The wizard provides the option of blocking ports completely or for a particular application only (e.g. your MP3 player software).
- **File/printer sharing:** If you permit access, you have the option of using shared folders and printers on the network. At the same time other computers and users on the network can access your shared data (where set up for this).
- **Allow or block domain services:** A domain is a type of classification directory for computers on a network that allows the computers linked to the network to be managed centrally. Enabling for domain services in untrustworthy networks should generally be denied.
- **Shared use of the Internet connection:** If your system connects directly to the Internet, you can specify whether all computers on the network should have access to the Internet via a computer connected to the Internet or not. Such Internet connection sharing can usually be enabled for a home network.
- **Allow or block VPN services:** VPN is an abbreviation for Virtual Private Network and refers to the option of exclusively linking computers to one another, thus setting up a sort of direct connection between them. To enable VPN services to function, they must be approved by the firewall.
- **Advanced Rule Set Editor (expert mode):** This allows you to move from the rule wizard to the advanced editing mode. For further information on the advanced editing mode, see the section entitled [Using the advanced editing mode](#).

## Using the advanced editing mode

The advanced editing mode allows you to set highly specific rules for the relevant network, although you will need a certain level of knowledge of network security for this. You can of course create all the rules here that can be created using the rule wizard, but advanced settings can also be made.

The following configuration options are available here:

- **Name:** This allows you to change the name of the current rule set if required. The rule set will then be displayed under this name in the list within the Rule sets area and can be combined with networks identified by the firewall there.
- **Stealth mode:** Stealth mode (meaning: hidden, secret) is used for not answering requests to the computer that verify the relevant port's accessibility. This makes it difficult for hackers to obtain system information in this manner.
- **Action if no rule applies:** Here you can specify whether access to the network is generally allowed, denied or regulated on request. Any special rules for individual programs defined by the firewall's learning function are applied.



- **Adaptive mode:** The adaptive mode supports applications that use feedback channel technology (e.g. FTP and numerous online games). These applications connect to a remote computer and negotiate a feedback channel with it, which the remote computer then uses to *reverse connect* to your application. If the adaptive mode is enabled, the firewall detects this feedback channel and permits it without querying it separately.

## Rules

The list of rules contains all the rules that are defined for this rule set. This means, for example, that selected programs can be authorised for numerous network accesses even if the network is classified as untrustworthy. The rules applicable here may have been created in various ways:

- Via the [Rule wizard](#)
- Directly using the [advanced editing mode](#) via the **New** button
- Using the dialog in the info box displayed when the [Firewall alarm](#) is triggered.

Of course, each rule set has its own list of rules.

Since the firewall rules are in part switched hierarchically, it is sometimes important to note the rank of each rule. For example, a port that you have granted access to may be blocked again because a certain protocol is denied access. To modify the rank of a rule in the sequence, highlight it with the mouse and use the arrow buttons under **Rank** to move it up or down the list.

If you create a new rule using the advanced editing mode, or modify an existing rule using the **Edit** dialog, the **Edit rule** dialog appears with the following setting options:

- **Name:** For default and automatically generated rules, this displays the program name to which the relevant rule applies.
- **Rule enabled:** You can disable a rule without actually deleting it by deactivating the checkbox.
- **Note:** This indicates how the rule was created. Next to rules preset for the rule set it says "Default rule"; next to rules that arise from the dialog for the [Firewall alarm](#) it says "generated in response to alert"; and for rules that you generate yourself via the advanced editing mode you can insert your own comment.
- **Direction:** This setting specifies if the selected rule applies to inbound or outbound connections, or to both inbound and outbound connections.
- **Access:** This specifies if access is to be permitted or denied for the relevant program within this rule set.
- **Protocol:** This allows you to select the connection protocols you want to permit or deny access. You can generally block or enable protocols or link usage of a protocol to the use of one or more specific applications (**Match to applications**). Similarly, you can use the **Match to Internet service** button to specify the ports that you do or do not wish to use.
- **Time window:** You can also set up time-related access to network resources to ensure, for example, that the network can only be accessed during your normal working day and is blocked at all other times.
- **IP range:** It is advisable to regulate network use by restricting the IP address range, especially for networks with fixed IP addresses. A clearly defined IP address range significantly reduces the risk of attack from a hacker.

# Backup

As everyday life becomes increasingly digitised, including the use of online music services, digital cameras and email, backing up your personal data becomes ever more important. In case there is a hardware error, an accident or damage from viruses or hacker attacks, you should take care to regularly backup your personal documents. The G DATA software takes care of this for you and protects your critical documents and files, without you constantly needing to think about this.

## Backup and restore

As soon as a backup job has been set up via the **New job** function, you can directly control and edit it via the following icons:



**Restore:** You can use this to restore data that has been archived in the backup to your system. How the restore works is explained in the section entitled [Restore backup](#).



**Backup:** You can use this to start the backup process for the defined backup job immediately and out of sequence, regardless of the preset schedule for this backup.



**Settings:** You can use this to change the settings for the relevant backup job that you made when initially setting up the backup job under [New backup job](#).



**Logs:** Here you can see all the processes carried out by this backup job. You will find entries on manual or scheduled backup processes carried out, information on any restores and, if appropriate, any error messages, e.g. when the target directory does not have enough storage space for the backup being run.

## New backup job



To assign a new backup job, please click on the **New job** button.

## Select files/hard drives/partitions

The backup wizard will now ask you what type of backup you want to run.



**File backup:** This involves backing up specific files and folders selected by you to an archive file.

In the directory view, simply select which files and folders you want to save. With a file backup it is generally recommended that personal files are saved and installed program files are not backed up. In the directory tree, you can open and select directories by clicking on the plus symbols. Their contents will then be shown in the file view. Each directory or file that you mark with a check will be used for the backup by the software. If not all files and folders in a directory are used for the backup, this directory is marked with a grey checkmark.



**Drive backup:** This involves a full backup of hard drives or partitions to an archive file.

## Select target

Here you can define the target or location to which the G DATA software should save the backup copy of the files and folders or hard drives and partitions. This can be a CD- or DVD-ROM drive, another hard disk, a USB stick, other removable media or a directory on the network.

**Archive name:** Here you can enter a meaningful name for the archive file to be created, e.g. *Weekly backup own files*, *MP3 backup* etc.

**New folder:** If you want to set up a new folder for the backup, select the storage location you want in the directory view, then click on the **New folder** button.

**Note:** Please ensure that the backup is not made to the same disk on which the original data is located. If this disk becomes defective, you will lose both your original and your backup data. The best thing to do is to keep the backup in a place that is remote from the original files, i.e. on a USB hard disk in another room or burnt to CD/DVD-ROM.

**Create cloud archive:** You can simply use popular Cloud services such as Dropbox, Microsoft OneDrive\*, TeamDrive\*\* or Google Drive to store your backup there. To do so, simply log in using the access data for your Cloud service, and your backup archive will be linked to the Cloud service.

**Note:** When backing up to the Cloud, you should ensure that your backup data is encrypted. In the [Options](#) under [New backup job](#) you can enable/disable data encryption.

**(\*) Note on OneDrive:** You can use OneDrive if you have integrated this service in Windows Explorer as a virtual drive. The archive is then generated as normal via the file directory, not via the **Create Cloud Archive** function.

**(\*\*) Note on TeamDrive:** You can select TeamDrive after using the TeamDrive software on your PC to configure and select a TeamDrive Space.

## Schedule

Here you can specify the frequency with which your selected data is backed up. You can also specify what type of backup should be run. The options are basically a full backup, where all the selected data is backed up in full, or a partial backup, where only the changes since the last backup are saved.

If you select **Manual**, the backup will not run automatically. Rather, it has to be specifically started by you via the program interface. Under **Daily**, you can use the Weekdays settings, for example, to specify that the computer should only carry out the tuning job on workdays or just every other day, or on weekends only, when it is not being used for work. You can also define weekly and monthly backups.

**Do not run when in battery mode:** To prevent a backup process from being suddenly interrupted by the notebook battery running out, you can specify that backups can only be run when the notebook is connected to the mains.

### Run full backup

Under **Run full backup**, just enter how often, on which days, and at what time the backup should take place. A backup of all data that you selected under [Select files/hard drives/partitions](#) will now be made automatically according to the frequency you entered.

**Warning:** Scheduled backups do not work with CD-ROMs or DVD-ROMs since user intervention may be required for changing a blank disk.

In the **Delete older archives** section you can define how to use the G DATA software with backups that already exist. The G DATA software archives your data to a separate file with the file extension ARC. Having existing backups that have not been overwritten naturally increases the security of your data since, in the event that the current archive should be corrupted, an older archive is available so you do not lose all the data. In general, however, archives require a lot of space on data carriers, so you should beware that you do not accumulate too many archive files. It is a good idea to set a maximum number of backups to store on your backup medium under **retain full backups**. The oldest archive will then be replaced by the current archive.

If you have checked the box next to **Create partial backup(s)**, the software will only run partial backups following the first full backup. These are significantly faster when backing up, but it may take longer if they have to be used to restore a full backup. Another disadvantage of partial backups is the comparatively greater storage space requirement, as data in the full backup that is no longer required will not be directly deleted. However, after the next full backup, the full and partial backup datasets will be synchronised and the data volume will again be the same as for a full backup.

### Run partial backups

Partial backups serve to speed up data security. Instead of using all data for a backup, a partial backup adds to an existing full backup and only backs up data that has changed since the last full backup. This way you still get a complete backup of your data set, but the backup process itself is significantly faster.

**Differential/Incremental:** With a differential backup all data that has been added or modified since the last full backup is saved. It is always added to the last full backup. This saves time and storage space compared to a new full backup. An incremental backup goes one stage further and backs up files that have been modified between one partial backup and another. The disadvantage of this is that multiple archives are required for a restore.

## Options

You can change general backup options in the Options area. In general, you do not have to make any changes here since the G DATA default options cover most application scenarios.

### General archive options

In the General archive options, you have the following settings options:

- **Limit archive size:** If you store archives on CD-, DVD-ROM or other writable media, it is important that the G DATA software limits

the size of the archive files. Here, you can choose from default sizes enabling you to retrospectively store the archive data on CD, DVD or Blu-ray discs. When the archive reaches the maximum size specified here, it is split and the backup information is spread across two or more archive files.

- **Create multisession CD/DVD:** If you select this option, you create backup CDs or DVDs that are rewritable. Doing so does not delete the content previously saved – it just enhances it with the new content.
- **Delete temporary archives:** This option should generally be enabled. After a certain number of backup operations, temporary archives require a lot of space on your hard disk and are no longer needed after their temporary use.
- **Copy restore program files:** If you activate this function, in addition to the archive data a program is also installed in the storage area of your data backup that you can use to restore your data without using installed G DATA software. To use this function, start the *AVKBackup* program or *AVKBackup.exe* from the CD/DVD ROM.

The restore program is only copied with it onto CD/DVD-ROM. This is not the case for backup copies to removable media (USB stick, external hard disk).

If you have installed the G DATA software on the computer on which the restore is due to take place, please do not execute the restore with the restore program on the CD/DVD-ROM. Instead, use the function [Import archive](#).

- **Check files for viruses before archiving:** If the AntiVirus module is installed, you can check your data for viruses before it is stored in the backup archive.
- **Check archive after creation:** The purpose of this function is to check the archive for completeness and correctness once it has been created.
- **Encrypt archive:** If you want to protect archived files from external access, you can assign a password to them. In this case, the data can only be restored with this password. You should memorise this password or write it down and put it somewhere safe. Your archive data cannot be restored without the password.
- **Integrity test with differential backup:** The purpose of this function is to check a partial backup for completeness and correctness once it has been created.
- **Integrity check when restoring from a hard drive:** This function is used to check that data has restored correctly after a restore. **Directory for temporary files** involves the storage area for data that the G DATA software only temporarily writes to your hard disk. If there is insufficient space on your standard partition, this is where you can change the partition and the temporary storage location for these files.
- **Use Windows volume shadow copy:** If this option is disabled, no image of the system partition can be created during normal operation.

## User details

To be able to carry out scheduled backups at all, you must check the box next to the **Run job as** option and enter the access data for your Windows user account there. This input is required so the backup can be scheduled to run even when you are not logged on as a user.

## Compression

In the Compression area, you can determine if your archives should be strongly or weakly compressed.

- **Good compression:** the data is strongly compressed for the backup. This saves you backup storage space, but the backup itself will take longer.
- **Balanced compression:** the backup is not so strongly compressed, but it will be executed more quickly.
- **Fast execution:** data is not compressed, so the backup is executed quickly.

## Exclude files

In general, the G DATA software saves files on the basis of their file format. On your computer system, however, corresponding file formats also exist in areas that are managed automatically and are not relevant for backup because the respective files are only stored temporarily (e.g. to speed up the display of pages from the Internet). To ensure that the G DATA software does not accidentally archive these files as well, you can exclude them by setting the corresponding checkmark.

- **Temporary directory with files:** If this option is selected, the temporary folders and any subfolders and files located there will not be included in the backup.

- **Temporary Internet directories with files:** If this option is selected, the folders for caching websites and any subfolders and files located there will not be included in the backup.
- **Thumbs.db:** If this option is selected, the thumbs.db files created automatically by Windows Explorer will not be included in the backup. These files are used to manage thumbnails for slideshows, for example, and are generated automatically from original images.
- **Temporary files (file attribute):** If this option is selected, the files with the system-assigned temporary file attribute are not included in the backup.
- **System files (file attribute):** If this option is selected, the files with the system-assigned system file file attribute are not included in the backup.
- **Exclude file type:** You can use this function to define file extensions that should be excluded from your backup. To do so, proceed as follows: Under **File type** (e.g. \*.txt), enter the file extension or file name that you want to exclude. Now click **OK**. Repeat this process for all other file types and file names that you want to exclude, e.g. picasa.ini, \*.ini, \*.bak etc. The asterisk and the question mark can be used as wildcards here. Wildcards function as follows:

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. In order to check various spreadsheet formats (for example, \*.xlr, \*.xls), simply enter \*.xl?. In order to check files of different file types but that have a file name that begins with the same string, you could enter text\*.\* for example.

## Reset to default

By clicking this button, you accept the options that have been defined as the default options for the G DATA software. That is, if you accidentally entered incorrect options for creating backups and you do not know how to correct them, click the **Reset to current default options** button.

## Restore backup



Here you can restore your original files using saved backup data in the event of data loss. To do this, simply click on the **Restore** button.

A dialog now appears where all the saved backup processes for the relevant backup job are listed.

Select the backup you want here (e.g. the last backup run if you want to restore documents recently deleted by accident) and press the **Restore** button.

You now have the option of defining what type of restore you want:

- **Restore full backup:** All files and folders backed up by this backup are restored.
- **Only restore selected partitions/files:** Here you can see a directory view of your backup, where you can specifically select which files, folders or partitions you want to restore and which you do not. In the directory tree, you can open and select directories by clicking on the plus symbols. Their contents will then be shown in the file view. Each directory or file that you mark with a check will be restored from the backup. If not all files in a directory are checked, this directory is marked with a grey checkmark.

Finally you can specify whether the files should be restored in their original directories or not. If the files should be saved somewhere else, you can if necessary select a folder under **New folder** where they will be stored. Under **Password** enter the access password if you have compressed your data backups as password protected files when you saved them.

If you restore files to the original directories, you have the following options for only retrieving files that have changed:

- **always overwrite:** In this setting, the files from the data backup are always seen as more important than the data that is still in the original directory. If you set a checkmark here, any data that may remain is completely overwritten by the data in the archive.
- **if size has changed:** With this setting, existing data in the original directory is only overwritten if the original file has been changed. Files where the size remains unchanged are skipped. In this way the data restore might run more quickly.
- **if the time "Modified on" in the archive is more recent:** Here, files in the original directory are always replaced with copies from the archive if they are newer than the data in the archive. This may also speed up the data restore because it can ensure that only changed data rather than all files have to be restored.

- **if the time "Modified on" has changed:** Here, the data in the original directory is always replaced if the modification date has changed compared to the archived files.

Now finish by clicking on the **End procedure** button to run the restore according to your specifications.

## Actions

You can manage and maintain your data backups and more in this area.

The following tools are available for this purpose:

### Burn archive to CD/DVD retrospectively

You can burn backup files to CD or DVD at a later date. To do this, simply choose the project you want to burn in the dialogue box displayed and then click the **Continue** button.

Choose which drive you want to burn the data backup on.

The following options are available:

- **Check data after burning:** if you set a checkmark here, the burned data is checked again after the process of burning. This takes a bit longer than a burning process without a check but is generally recommended.
- **Copy restore program files:** If you activate this function, in addition to the archive data a program is also installed in the storage area of your data backup that you can use to restore your data without using installed G DATA software. To use this function, start the *AVKBackup* program or *AVKBackup.exe* from the CD/DVD ROM.

Click the **Burn** button to start the burning process. Once the burning process is complete, the backup CD/DVD is ejected automatically.

**Note:** Of course, the backup data is not deleted from the original data medium after the burning process. Retrospective burning to CD/DVD is an additional backup.

## Import archive

To restore archives and data backups located on a drive that is not managed by the G DATA software, please use the **Import archives** function. Here, a dialogue box opens in which you can search for the required archive files with the extension *ARC*, e.g. on a CD, DVD or on the network. Once you have found the archive you want, please set a checkmark and then click the **OK** button. A message window tells you that the archive has been imported successfully. If you then want to use this archive to restore data, simply go to the [Restore](#) area in the G DATA software, select the backup you want and start the restore.

**Note:** Archive files generated by the G DATA software have the file extension *ARC*.

## Create boot medium

In order to be able to restore backups even when the G DATA software is not installed, you can create a CD/DVD or USB stick that contains special software that you can use to be able to restore data. To restore backups in this way, start the boot medium and select the program *AVKBackup* or *AVKBackup.exe* there. You can now select the backup you want and start the restore.

**Note:** How to create a boot medium is explained in the section entitled [Boot medium](#). The boot medium does two jobs for the G DATA software. You can use it to restore backups, and you can use the boot scan to check your computer for viruses before starting Windows.

# Password Manager

You can use the Password Manager as a handy plug-in for your browser to easily manage passwords.

The Password Manager supports the latest generation of the following browsers:

- Google Chrome
- Mozilla Firefox
- Microsoft Internet Explorer

**Note:** Please note that the functionality of the Password Manager may be restricted depending on your browser settings (e.g. data protection settings).

Please set up a password safe first and then install the plug-in for the browser of your choice. You can of course install the password safe on all compatible browsers.


## Setting up a new safe and installing the plug-in

Click on the **Password Safe** entry. A dialog box now opens in which you can set up a new safe by selecting **Create new safe**.

To do so, enter a password, confirm it, click on **Create safe** and the safe is set up. The reminder phrase will help you recall a forgotten password.

The safe is now set up. On the right hand side of the program window, you can select the browser in which you want to set up the Password Manager plug-in. To do so, simply click on the relevant browser name and the plug-in is installed.

The next time you open the browser, you may be asked whether you want to use the new plug-in. Please confirm this for the G DATA Password Manager.

 You will now see the following icon in the browser's toolbar. You can use the Password Manager by clicking on the icon.


To do so, please enter your password in the dialog that appears and click on **Unlock**. Using the browser plug-in is explained in the following [chapter](#).


## Using the browser plug-in

 You can use the Password Manager by clicking on the following icon in the browser's toolbar.


**Note:** Please note that you may not be able to use the plug-in depending on your privacy settings (e.g. save the history). If you have problems with the plug-in, please check your browser settings first.


To do so, please enter your password in the dialog that appears and click on **Unlock**. The following areas are now available:

 **Favorites:** You can use this function to quickly call up password-protected websites that you use regularly.

 **Logins:** Here you can manage logins for password-protected websites.

 **Contacts:** The contact data entered here can be used for automatically filling out forms such as delivery addresses.

 **Notes:** You can save additional notes with password protection here.

 **Settings:** To close the Password Manager again, please click on **Lock**. If you click on Settings, you can easily manage favorites, logins, contacts and notes in dialog boxes. You can use the password generator to automatically generate a secure password and reuse it directly via the clipboard.

You can add, edit and delete entries in the Password Manager in the following way.



**New entry:** By clicking on this button you can compose a new entry and add all the necessary data for logins, contacts or notes in the relevant dialog boxes.



**Save entry:** By clicking on this button the entry is saved and displayed in the browser plug-in's quick selection list.



**Delete entry:** Use this to delete entries you no longer need.



# Tuner

From automatically memorising Windows updates to regular, scheduled defragmentation and regular removal of unnecessary registry entries and temporary files, the tuner is a handy tool for making your Windows system much faster and more manageable.

You can either tune your computer manually at the push of a button or run regular scheduled tuning jobs.



**Last tuning process:** Here you can see the last time that your computer was tuned. To start a new tuning job, click on the **Perform tuning run now** entry here. As soon as you start the tuning run, a progress bar will display the current status of the job.



**Automatic tuning process:** If you want to automate the tuning of your computer, you can click on the **Enable automatic tuning process** entry here to generate a corresponding scheduled job. To set up automatic tuning processes, select the **More settings** option.



**Configuration:** In this [area](#) you can select all the modules that the tuner should use for a tuning process. Selected modules are then either started automatically as a scheduled event (see [Scheduling](#)) or manually. To activate a module simply double-click it. You can optimise the following main tuning areas as you want here:

- *Security:* Various functions that download data automatically from the Internet are only of use to the provider and have no benefit for you. These functions may often leave you vulnerable to malware. With these modules you can protect your system and keep it up-to-date.
- *Performance:* Temporary files, e.g. backup files that are no longer required, log files or installation files that still take up disk space following the installation slow down your hard drive and take up valuable disk space. Moreover processes and file links that are no longer required can significantly slow down your system. You can use the modules listed here to remove this superfluous load from your computer and speed the computer up.
- *Data protection:* This summarises the modules that deal with protecting your data. Traces that are created unintentionally while surfing or using the computer in general and that contain a lot of information about your user behaviour, or even important data and passwords, are deleted here.



**Restore:** The software creates a restore point each time a change is applied. If one of the executed tuning actions leads to unwanted results, you can undo this action and restore your system to the status before the respective change. For more information see the section entitled [Restore](#).



**Browser Cleaner:** The G DATA Browser Cleaner is capable of blocking or removing unwanted program components and add-ons. These programs are often installed with free software and can change browser settings or even spy on data. For more information see the section entitled [Browser Cleaner](#).

## Restore

The software creates a restore point each time a change is applied. If one of the executed tuning actions leads to unwanted results, you can undo this action and restore your system to the status before the respective change.



**Select all:** If you want to reject all the changes made by the tuning module, you can use this to select all the restore points and then click on the **Restore** button.



**Restore:** If you want to reject just specific changes made by the tuning module, you can use this to select the restore points you want and then click on the **Restore** button.



**Selective delete:** Restore points that you no longer need can be removed with this button.

# Browser Cleaner

The G DATA Browser Cleaner is capable of blocking or removing unwanted program components and add-ons. These programs are often installed with free software and can change browser settings or even spy on data. You can use the Browser Cleaner to view these unwanted programs ("PUP" = Potentially Unwanted Programs) in the Internet Explorer, Firefox and Google Chrome browsers and specify for yourself if these should only be disabled or should be completely removed. Disabling the add-ons can be reversed again at any time.

**Note:** The G DATA Browser Cleaner works with Microsoft Internet Explorer, Mozilla Firefox and Google Chrome and enables effortlessly easy management of all installed browser extensions. With a click of the mouse, all plug-ins in the list can be disabled or removed to free the browser of unwanted extensions. The tool optionally displays all plug-ins categorized as safe, so you can quickly and easily distinguish the unsafe or unwanted extensions. The G DATA Browser Cleaner is included in the comprehensive G DATA Total Security solution and is always available to users of this.

# Parental controls

You can use parental controls to regulate surfing behavior and computer use for your children.

Under **User** select a user logged onto your computer and set up the appropriate restrictions for him/her. You can use the [Create new user](#) button to set up new accounts on your computer directly (e.g. for your children).

- **Parental controls for this user:** Here you can switch parental controls for the user selected above on or off.
- **Prohibited content:** A dialog window opens where you can block specific web content for the user currently displayed. Click on [Edit](#) to specify the forbidden content for the relevant user.
- **Permitted content:** A dialog window opens where you can permit specific web content for the user currently displayed. Click on [Edit](#) to specify the permitted content for the relevant user.
- **Monitor Internet usage period:** This allows you to specify for how long and at what times the selected user can access the Internet. Click on [Edit](#) to specify the usage times for the relevant user.
- **Monitor computer usage time:** This allows you to specify for how long and at what times the selected user can use the computer. Click on [Edit](#) to specify the usage times for the relevant user.

**Settings:** This is where you can adjust the basic operational settings for the parental controls and adapt them to your individual requirements.

## Create new user

Click the **Create new user** button. Enter the user name and password for the relevant user in the dialogue box.

**Note:** To make a password as secure as possible, it should be at least 8 characters long and include upper and lower case letters as well as numbers.

You will now see the new user name under **User**; a Windows user account is created for this user at the same time. This means that parental controls are automatically activated for the person whose user name was used to log on when Windows was started, and that this person's settings will apply. By double-clicking the Settings area, you can select the settings for a particular user, for example: to block **Forbidden content** or to allow only **Permitted content** or to specify whether the **Internet usage time** or **Computer usage period** should be monitored for this user.

## Forbidden content

Opens a dialogue window in this area where you can block specific web content for the user currently displayed. Check the categories you wish to be blocked. Click on **OK** and the websites that fit the blocking criteria will be blocked.

If you click on the **New** button, a dialog box opens where you can define your own blocking criteria (also called blacklists). To do this, first give the name and, if you want, any additional information about the filter you are creating.

Then click on **OK** to open a new window which lets you list the content you'd like blocked by this filter.

Add a term under **Filter** that is to be blocked, and under **Search location** indicate the parts of a website that should be searched for the term.

Here, you have the following options:

- **URL:** If you check "URL" it will search for the term that should be blocked in the web address. For example, if you want to block websites like *www.chatcity.no*, *www.crazychat.co.uk* etc., you can simply set **chat** as a *filter*, check the **URL** option and click on the **Add** button. This way, you can block all websites in which the word *chat* appears in the domain name (i.e. the website address).
- **Header:** If you check "Header" it will search for the term that should be blocked in the website's title. This is the area displayed, for example, when you want to bookmark a website in your "Favorites" list. For example, if you want to block websites like *Chat City Detroit*, *Teenage Chat 2005* etc., you can simply set **chat** as a *filter*, check the **Title** option and click on the **Add** button. This way, you can block all websites in which the letter combination *chat* appears in the title.
- **Meta:** The meta tags are text items concealed on websites designed to make search engines list the websites more effectively or more frequently. Search terms like *sex* or *chat* are often used here to increase the number of hits a website receives. If you want to block websites in which *chat* appears among the meta tags, you can simply set **chat** as a *filter*, check the **Meta** option and click on the **Add** button. This way, you can block all websites in which the letter combination *chat* appears in the meta tags.

- **In entire text:** If you want to check all readable content of a website, just add a term that should be blocked – for example, *chat* – then check the **In entire text** option and click on the **Add** button. This way, you can block all websites in which the word *chat* appears anywhere in the website text.

Websites that accidentally get filtered can be removed from the list using the Exceptions function. To do so, just click on the **Exceptions** button and enter the relevant site there.

**Note:** You can edit and delete your own filters as required in the **Personal Filters** area. For more information, see the section [Personal filters](#).

## Permitted content

Opens a dialogue window where you can permit specific Internet content for the user currently displayed. Select the categories you want to permit by checking the relevant boxes. Now click **OK** to permit access to the websites relating to the criteria you want.

If you click on the **New** button, a dialog box opens where you can define your own permitted content (also called whitelists). There you can give a name (and a short description if you want) to your personally created filter.

Now, click **OK**. A dialogue window will open in which, for example, you can create a whitelist of websites suitable for children.

Under **Filter**, enter the domain name components you wish to permit. If, for example, you want to permit access to a website with child-friendly content, you can enter e.g. *www.nick.com* to allow access to this website. Now indicate in the **Description** field what is contained on this website (e.g. *Nickelodeon - child-friendly website*) and enter the site's exact web address under **Link to website**. The description and link to the website are important if, for example, your child tries to access a website that you have not permitted. Instead of an error message, an HTML website will appear in the browser listing all the websites on the whitelist and a description. This allows your child to directly access the websites he or she is permitted to visit. Once you have added all the entries, click **Add** and the whitelist will be updated to include these details.

**Note:** The filter also searches for parts of domain names. The results can vary depending on what you enter in the filter. Broader or stricter criteria can be useful here, depending on the website.

## Monitor Internet usage time

This allows you to specify for how long and at what times the selected user can access the Internet. To do this, check the box next to **Monitor Internet usage period**. You can now specify how long the user can access the Internet in total per month, how long per week and how many hours on particular days of the week. This means that e.g. weekends for school children can be handled differently from weekdays. You can simply set the relevant periods under **Days/hh:mm**, where for example the entry *04/20:05* would mean permission to use the Internet for 4 days, 20 hours and 5 minutes.

**Note:** When there are conflicting settings for Internet usage, the smallest value is always used. So, if you set a time limit of four days per month, but a weekly limit of five days, the software will automatically limit Internet usage to four days.

If users try to access the Internet beyond their permitted amount of time, a message appears telling them that they have exceeded their allotted time.

## Block periods

With the **Block periods** button, you can open a dialogue box where you can completely block certain time periods during the week - in addition to limiting the computer usage. The blocked time periods are shown in red; the allowed time periods are shown in green. In order to allow or block a time period, simply highlight it using the mouse. A context menu then appears next to the cursor in which you have two options: **Approve period** and **Block period**. If users try to access the Internet during the blocked periods, an information screen will appear in the browser informing them that they do not have Internet access during that period.

## Monitor computer usage period

This allows you to specify for how long and at what times the selected user can use the computer. To do this, set the checkmark for **Monitor computer usage period**. You can now specify how long the user may use the computer for in total per month, how long per week and how many hours on certain weekdays. This means that e.g. weekends for school children can be handled differently from weekdays. You can simply set the relevant periods under **Days/hh:mm**, where for example the entry *04/20:05* would mean permission to use the computer for 4 days, 20 hours and 5 minutes. You can use the **Display warning before time expires** button to automatically inform the user shortly before the computer is shut down so that he/she can save his/her data beforehand. Otherwise data losses may occur if the computer is shut down without warning.

**Note:** In the context of the computer usage entries, it is always the smallest value that is used. That means, if you specify a restriction of four days for the month but allow e.g. five days during the week, the software automatically caps the user's

computer usage at four days.

## Block periods

With the **Block periods** button, you can open a dialogue box, where you can, in addition to limiting the computer usage, completely block certain time periods during the week. The blocked time periods are shown in red; the allowed time periods are shown in green. In order to allow or block a time period, simply highlight it using the mouse. A context menu then appears next to the cursor in which you have two options: **Approve period** and **Block period**.

## Personal filters

In this area you can modify the whitelists (permitted content) and blacklists (prohibited content) you have compiled and create entirely new lists manually.

List types differ fundamentally from one another, as described below:

- **Permitted content:** If you set up a whitelist for one of the users selected above, the relevant user can only view websites specified in this whitelist. As the administrator, you may set up the whitelist as required or select an appropriate list for a user from a number of predefined whitelists. A whitelist is particularly suitable for allowing younger children restricted Internet access, enabling them to use websites with beneficial educational content only.
- **Prohibited content:** A blacklist allows you to block access to selected websites for a specific user. Otherwise, the user has free access to the Internet. Please note that this function allows you to block specific pages but that identical content may still be accessible on other websites. In this regard, a blacklist of Internet addresses can never provide complete protection against unwanted content.

The following buttons can be used to edit the exclusion lists:

- **Delete:** The **Delete** function enables you to delete the selected lists quickly and easily with the mouse.
- **New:** Use this to set up a completely new blacklist or whitelist. The procedure for using this function is the same as that described in the sections entitled [Prohibited content](#) and [Permitted content](#).
- **Edit:** This allows you to modify the contents of an existing list.

## Settings: Log

You can use this area to change the basic settings for the information in the log area. In this manner, you can specify whether violations of allowed and/or prohibited content should be logged or not. If contents are logged, you can view the logs of different users in the log area.

Since log files grow considerably during regular use, you can have the Parental Controls setting **Alert when file reaches \_\_\_\_ KB** remind you that the log file has exceeded a certain size, and then delete it manually in the [Log](#) area, under **Delete logs**.

# Encryption

The encryption module acts like a safe for protecting sensitive data. A safe can be e.g. used as an extra drive like an additional hard disk partition and is very easy to work with.

You have the following options for creating and managing safes:

- **Update:** If you have opened or closed safes outside of the file safe module in the meantime, it is recommended that you click on **Update** to bring the status display for the safes managed by the encryption module fully up to date.
- **Open/close:** Here you can open and close safes that are located on your computer and on attached storage media. Please note that you need the password you entered for the safe during setup to open the safe. Safes can be closed here without a password.
- **Create new safe:** You can use this function to set up a new safe. To do this, a wizard will appear that will help you set up the safe. For more information, see the section [Create new safe](#).
- **Create mobile safe:** As soon as you have created a safe, you can also turn it into a mobile safe, i.e. you can configure it so that you can use it on a USB stick or even send it via email. For more information, see the section [Create mobile safe](#).
- **Delete:** In safe administration you can find an overview of all safes located on your computer and on attached storage media. You can also delete safes that are no longer needed here. Please note that safes can also be deleted here without knowing their passwords. Therefore you should ensure that you really no longer need the content of the safe you are about to delete.

## Create new safe

If you want to create a new safe, there is an interactive dialog to support you. Click on the **Next** button to continue.

## Storage location and size of the safe

Now enter where the safe should be stored and what size it should be.

**Note:** The safe is actually a protected file that works like a hard drive partition when it is open, i.e. you use Storage location to create a safe file in a location of your choice on the hard disk. Your data is encrypted and saved there. If you open the safe and work with it, you can still edit, delete, copy and move files and directories in it as with a normal hard disk or hard drive partition.

### Storage location

Please select the data medium (e.g. local data medium (C:)) on which the safe should be created.

**Note:** Safes created in a protected directory are only visible on your computer if the G DATA software has been installed on your computer. If you need to uninstall the software, the data safes that have been created will no longer be visible.

### Safe size

Then select a safe size by positioning the slide control as appropriate. You then have as much space as remains available in the storage location you have chosen. However, there should generally be at least 2 GB more than the maximum size available so your computer is not slowed down in other areas due to lack of storage space.

**Note:** The button to the left of the slide control for the safe size gives you the option of fast selection. You can use this to e.g. define the size of the safe precisely or make it the right size for burning onto a CD, DVD or Blu-ray if necessary.

Now click on the **Next** button.

## Safe parameters

In this dialogue window you can make the following entries and settings:

- **Safe designation:** The name under which the safe is managed by the G DATA software.
- **Description:** an additional short description that contains e.g. information on the safe contents.
- **File system:** here you can define whether the virtual drive creating the safe uses the FAT or NTFS file system. Generally you should leave the entry here as **Automaticselection**.

- **Automatically select safe drive:** the safe is displayed on your computer like a hard disk drive. You can either allocate a fixed drive designation letter for the safe or let the system select one automatically. Automatic selection is generally recommended here.
- **Assign drive:** this option is only available to you if you are not letting the software automatically select the safe drive.

Now click on the **Next** button.

## Safe access

Here you can allocate a password for a safe. Click on the **Add** button.

Now enter the password you want in the dialog box that appears under **Password** and **Repeat password**. The password is only accepted if both entries are identical. This is intended to prevent you from e.g. making a mistake that you cannot reproduce when allocating a password.

Click on **Add** to activate the password, then on **Next** to finish configuring the safe.

**Note:** When creating a safe you can allocate a number of different passwords and use them to define different authorizations. For example, you can create a safe where you can read and change files, but other people using another password only have the option of reading the contents of this safe, not amending them.

If you select this after creating a safe and click on the **Permission** button, you have the following settings options:

- **Edit Autostart:** Every safe contains a directory called Autostart. If this option remains set to Yes, all executable files located there will be automatically started when the safe is opened.
- **Open in "Read only" mode:** A user who logs on using the read only access method will not be able to save or change files stored in the safe. He/she can only read it.
- **Open as removable medium:** The G DATA software opens file safes in Explorer as local hard disks. Check this option if you want the safe to be displayed as a removable data carrier in the system.
- **Shared usage:** Selecting this option enables shared use of the safe directory for other computers in the network. Alert: With this setting you can access the safe without needing to enter a password. At this point we recommend you think carefully about shared use of the safe. Shared usage of the safe for all network participants does not make sense at this point because the data would be accessible to everyone.
- **Close safe after user log off:** This option should generally be enabled because, if the safe stays open after the user logs off, other users can see the contents of the safe.
- **Auto safe:** All safes with this attribute can be opened with one command.

## Safe configuration

The safe creation wizard tells you about setting parameters in the last step. If you want to change these settings, please click the **Back** button. If you are happy with the settings, please click **Create**.

The virtual and encrypted file safe is created on your computer's hard drive. By finally clicking on the **Finish** button the safe is created and can be opened directly if you want.

## Create mobile safe

As soon as you have created a safe, you can also turn it into a mobile safe, i.e. you can configure it so that you can use it on a USB stick or even send it via email.

In the data safe overview, select a safe that has been created and click on the **Create mobile safe** button. A dialog now opens that will help you create a mobile safe. Click on **Next** to start this process.

## Safe parameters

As with allocating safe parameters for standard safes, you have the option here of changing parameters. However, with mobile safes there are only limited setting options.

- **Automatically select safe drive:** The safe looks like a hard disk drive when it is open. You can either allocate a fixed drive designation letter for the safe or let the system select one automatically. Automatic selection is generally recommended here.
- **Link safe with data medium:** Here you can specify that the mobile safe can only be used with the USB stick or hard disk drive that you created it on, for example. If you do not link the safe to the data medium, you can e.g. send the safe file (recognizable by the file extension **tsnxg**) as an email attachment or move/copy it to another data medium.

## Medium

Specify here the medium on which you want to save the mobile safe. This can be e.g. a USB stick, an external hard disk or a CD/DVD.

**Note:** If you are saving a safe to a CD or DVD, this can of course only be opened and read. It is not possible to amend files and directories in the safe with this type of data medium.

## Safe size

Here you can find information on how much storage space the safe needs on the target data medium. If the storage space is too big, you can cancel the creation of the mobile safe.

**Note:** In addition to the actual safe size, there is an extra 6 MB of driver data so you can open the safe on a Windows system on which the G DATA software is not installed.

## Finish

Now finish creating the mobile safe by clicking on the **End procedure** button. If you want, you can now see in the file browser the file on your chosen storage medium where the mobile safe is located.

## Open mobile safe

If you want to open a portable safe on a Windows computer that does not have the G DATA data safe module, you can easily access the data by selecting the **start.exe** or **start** program file in the **TSNxG\_4** folder on the USB stick, mobile hard drive or CD/DVD. If you click on this, a dialog appears in which you can open the safe or (if already open) close it.

**Warning:** If the G DATA data safe is being used on a computer for the first time, the relevant driver data and program elements are now downloaded. A computer restart is then required. After restarting the computer, choose the **Start** or **Start.exe** entry again.

Now enter your password or use one of the other safe access methods.

The safe is now opened and the contents of the safe can be used.

After successfully logging in to the safe, the safe icon appears as an additional drive with a corresponding drive letter next to the local drives in Windows Explorer. Every mobile safe user can copy data from the safe onto the computer. When a mobile safe is used on a USB data carrier or Flash memory data carrier, any appropriately authorised user can copy safe data from the computer to the safe.

Closing the mobile safe is performed in the same way as opening it. Double-click the drive letter for the safe or choose a corresponding command from the context menu by using the right mouse button.


**Warning:** We recommend closing the safe once you have finished your work and before removing the portable data carrier. To do so, go to the removable data medium, open the G DATA directory and click on Start.exe. A dialog window then appears in which the safe can be closed.




# Autostart Manager

The Autostart Manager enables you to manage programs that are automatically started when Windows starts. Normally such programs are loaded on system start-up. However, when they are managed by the Autostart Manager, they can also be started with a delay or according to the workload of the system or hard disk. This makes system start-up faster and so improves the performance of your computer.

When you open the Autostart Manager, you can see a list on the left hand side of all autostart programs that are installed on your computer. These normally start without a delay, i.e. at the same time as Windows starts, which can cause your computer to start very slowly.

 Simply use the arrow icon to select the autostart programs that you want to start with a delay, thus smoothing the Windows start-up process. This will make your Windows operating system load and be ready for use significantly faster.

 If you want an autostart program to start without a delay again, simply move it back from the **Autostart with delay** folder to the **Autostart without delay** folder.

## Set delay

If you have a program in the Autostart with delay folder, you can easily specify how many minutes the start of this software should be delayed for. Just click on the program and select the period of time you want in the Delay column.

The following options are available:

- **Do not launch:** The application is managed by the Autostart Manager but is not started on the next system restart. It remains inactive.
- **1 - 10 minutes:** The application starts after the number of minutes selected here.
- **Automaticstart:** The application starts automatically according to the load on the CPU/hard disk. This means that the next autostart application will only start when the system load caused by other autostart applications or processes starting has reduced again.

## Properties

If you double-click the entry for a program in the Autostart Manager lists, you will see detailed information on the software being managed.

# Device control

You can use device control to specify for your computer which storage media are permitted to read and/or write data. Hence for example you can prevent private data from being moved to a USB stick or burned to a CD. Furthermore, with removable data carriers such as USB sticks or external USB hard drives, you can specify precisely which removable data carriers can be used for downloading data. This means for example that you can use your own USB hard drive to back up data, but other hard drives are not granted access.

In this overview you can see what effects the device control settings will have for the user concerned. You can use the "Edit rules" button to adjust the settings for the device and the user how you want.

**USB Keyboard Guard:** Our software will also protect you as of now against a new threat: infected USB sticks that pretend to be a keyboard to your operating system and so are able to smuggle in malware. When you insert a USB device, the software lets you know when your system thinks it is a new keyboard. You can then confirm that it is by entering a PIN, or say that it isn't. Obviously the software notices all keyboards that are already approved and does not ask repeatedly.

# Settings

In the **Settings** area you can configure the relevant program module how you want. In general there is no need to make any changes at all here, as your G DATA software has already been optimally configured for your system during installation. The following general functions are available for the settings:



**Save settings:** You can save the settings you have made to a GDataSettings file. If you are using your G DATA software on multiple computers, you can use this to create settings on one computer, save them and load the settings file onto the other computers.



**Load settings:** You can use this to load a GDataSettings file you have created on this or any other computer.



**Reset settings:** If you have made a mistake when configuring your G DATA software, you can use this button to reset all of the software settings to the factory settings. When doing so you can specify whether you want to reset every settings area or just specific ones. To do this, simply tick the checkboxes for the areas you want to reset.

## General

### Security/performance

If you want to use virus protection on a slow computer, there is the option of improving the security level to the benefit of performance, thus improving the operating speed of the computer. In the diagram you can see what effect optimising the settings can bring.

- **Standard computer (recommended):** You have the complete protection of the G DATA software at your disposal. The two antivirus engines in the software work hand in hand. In addition, all read and write access on your computer is checked for malware.

**Engine:** Your G DATA software works using two antivirus engines. In principle, use of both engines should guarantee optimum virus protection results.

- **Slow computer:** In order not to compromise the processing speed of slower computers, your G DATA software can also work with just one engine. This is the only protection offered by numerous antivirus programs on the market that only work with one engine in the first place. This means that the level of protection is still good. Furthermore you can specify that scans are only carried out in monitor mode when write processes are being executed. This means that only newly saved data is checked, improving performance even more.
- **User-defined:** Here you can custom select whether you want to use both engines or just one engine and you can specify whether the monitor should be active when reading and writing, just when writing (executing) or not at all (not recommended).

## Password

By allocating a password you can protect the settings for your G DATA software. In this way another user of your computer cannot switch off e.g. the virus monitor or idle scan.

To allocate a password, please enter it in "Password" then "Re-enter password" to prevent typing errors. You can also enter a hint for the password under "Password hint".

**Note:** The password hint is displayed if an incorrect password has been entered. Hence the password hint should only enable you to infer the password.

**Note:** Such password protection represents enhanced protection of the software. You can achieve maximum security by working with multiple user accounts. Hence as administrator you should manage e.g. virus protection in your user account and other users (e.g. children, friends or relatives) cannot make changes via their user accounts with restricted permissions.

**Note:** If you no longer need a password for your G DATA software – e.g. after setting up different user accounts – you can use the "Remove password" button to remove the requirement to enter a password.

# AntiVirus

## Real-time protection

The virus monitor real-time protection continuously checks your computer for viruses; it controls read and write operations, and as soon as a program attempts to execute malware or spread malicious files it prevents it from doing so. The virus monitor is your most important protection! It should never be switched off.

The following options are available:

- **Monitor status:** Specify here whether the monitor should be enabled or disabled.
- **Use engines:** The software works with two engines, which are two essentially independent virus checking programs. Every engine by itself would already provide you with a high degree of protection against viruses, but it is precisely the combination of both engines that gives the very best results. You can accelerate the virus check in older and slower computers by using just one engine, but normally you should keep the setting **Both engines**.
- **Infected files:** If a virus is detected, you will be asked in the default setting how you want to deal with the virus and the infected file. If you would always like to perform the same action, you can set this here. The highest protection for your data is offered here by the setting **Disinfect (if not possible: place in quarantine)**.
- **Infected archive:** Here you determine whether archive files (e.g. files with the extension RAR, ZIP or PST) should be handled differently from normal files. However, please note that moving an archive to quarantine can damage it so that it can no longer be used after it is moved back from [Quarantine](#).
- **Behavior monitoring:** If behaviour monitoring is enabled, every activity on the system is monitored regardless of the virus monitor. This means that malware for which no signature yet exists is also detected.
- **AntiRansomware:** Protection against encryption Trojans.
- **Exploit Protection:** An "exploit" exploits vulnerabilities in popular software and can use them to take control of your computer in the worst case. Exploits can even come into effect when applications (e.g. PDF viewer, browser etc) are routinely updated. Exploit Protection protects you against such access – and proactively protects you against previously unknown attacks.

## Exceptions

By clicking on the Exceptions button you can exclude specific drives, directories and files from the scan and so significantly accelerate parts of the virus detection process.

To do this, proceed as follows:

- 1 Click the **Exceptions** button.
- 2 Click **New** in the **Monitor exceptions** window.
- 3 Now, select whether you want to exclude a drive, a directory or a file or a file type.
- 4 Underneath this, select the directory or drive you want to protect. In order to protect files, enter the complete file name in the entry field under File mask. You can also use wildcards here.

**Note:** Wildcards function as follows:

- The question mark symbol (?) represents individual characters.
- The asterisk symbol (\*) represents entire character strings.

For instance, in order to protect all files with the file extension .sav, enter \*.sav. In order to protect a special selection of files with sequential file names (e.g., text1.doc, text2.doc, text3.doc), enter text?.doc for example.

You can repeat this procedure as often as desired and also delete or modify the existing exceptions.

## Advanced

Furthermore, you can click the button **Advanced** to specify which additional tests should be performed by the virus monitor.

Normally you do not have to deal with any more settings here.

- **Mode:** Here you can specify whether files should be checked when run, when read or when written to and read. If a file is checked when written to, the check is carried out as soon as a new file or file version is created to see if an unknown process may have infected this file. Otherwise files are only checked when they are read by programs.
- **Monitor critical folders in particular:** You can use this function to specifically check especially critical folders, e.g. folders shared on the network, personal data or Cloud services (such as Microsoft Dropbox, OneDrive, Google Drive etc). After you have made your selection in the dialogue box, this is then always monitored in **Check read write access** mode – regardless of the settings you use for all other files, folders and directories. If you have selected the **Check read write access** mode for all files by default, the settings option for critical folders is greyed out.
- **Check network access:** If your computer has a network connection to unprotected computers (for example, other laptops), it is a good idea to check the network accesses to see if any malicious programs are being transferred. If you use your computer as a stand-alone computer without network access, you don't need to enable this option. If you have installed virus protection on each computer in the network, it is recommended that you turn off this option. Otherwise, some files will be checked twice, which negatively affects speed.
- **Heuristics:** In the heuristical analysis, viruses are not only detected by means of virus updates that you regularly receive from us online, but are also identified on the basis of certain characteristics typical of viruses. This method increases the level of security, but in rare cases may generate false alarms.
- **Check archive:** Checking compressed data in archives (these can be recognized by their file extensions such as ZIP, RAR or PST) is very time-consuming and can normally be omitted if the virus monitor is generally active on the system. To increase the speed of the virus check, you can limit the size of the archive files that are browsed to a specific value in kilobytes.
- **Check email archives:** Because the software already checks incoming and outgoing emails for virus infections, it is usually a good idea to omit regular checks of email archives since this process may take several minutes, depending on the size of the mail archive.
- **Check system areas during system start:** In general, system areas (e.g. boot sectors) in your computer should not be excluded from virus checks. You can specify here whether you want to run a check on system start-up or when media is changed (for example, a new CD-ROM). Generally you should have at least one of these two functions activated.
- **Check system areas during change of medium:** In general, system areas (e.g. boot sectors) in your computer should not be excluded from virus checks. You can specify here whether these should be checked on system start-up or whenever a media change occurs (new CD-ROM etc). Generally you should have at least one of these two functions activated.
- **Check for diallers/spyware/adware/riskware:** You can also check your system for dialers and other malicious programs with this software. These are e.g. programs that establish expensive, unwanted Internet connections, in which the potential for financial damage is no less significant than that of a virus. They may for example secretly record your surfing habits or even all the keyboard entries you make (including your passwords) and forward these to third parties via the Internet at the earliest opportunity.
- **Only check new or modified files:** If you activate this function, files that have not been changed for a long time and that were previously flagged as harmless are skipped. This provides a performance improvement in everyday work – without compromising security.

## Manual virus check

Here you can create basic program settings for Virus check.

However, in normal operation this is not required.

- **Use engines:** The software works with two engines – two virus checking programs optimized for one another. You can accelerate the virus check in older and slower computers by using just one engine, but normally you should keep the setting **Both engines**.
- **Infected files:** Has your software detected a virus? In the standard setting, the software now asks you what you would like to do with the infected file. If you would always like to perform the same action, you can set this here. The highest protection for your data is offered here by the setting **Disinfect (if not possible: place in quarantine)**.
- **Infected archive:** Here you determine whether archive files (e.g. files with the extension RAR, ZIP or PST) should be handled differently from normal files. However, please note that moving an archive to quarantine can damage it so that it can no longer be used after it is moved back from [Quarantine](#).

- **Pause the virus check at times of high system load:** A virus check should normally be carried out when the computer is not being used. If you then need to use the computer, the virus check is paused so that your computer can run at normal speed for you. This virus check will then carry on when you stop working.

## Exceptions

By clicking on the Exceptions button you can exclude specific drives, directories and files from the scan and so significantly accelerate parts of the virus detection process.

To do this, proceed as follows:

- 1 Click the **Exceptions** button.
- 2 Click on **New** in the **Exceptions window for manual computer scans**.
- 3 Now, select whether you want to exclude a drive, a directory or a file or a file type.
- 4 Underneath this, select the directory or drive you want to protect. In order to protect files, enter the complete file name in the entry field under File mask. You can also use wildcards here.

**Note:** Wildcards function as follows:

- The question mark symbol (?) represents individual characters.
- The asterisk symbol (\*) represents entire character strings.

For instance, in order to protect all files with the file extension .sav, enter \*.sav. In order to protect a special selection of files with sequential file names (e.g., text1.doc, text2.doc, text3.doc), enter text?.doc for example.

You can repeat this procedure as often as desired and also delete or modify the existing exceptions.

**Use exceptions for the idle scan as well:** During a manual virus check the computer is scanned for viruses in a targeted manner and should not be used for other tasks, whereas the idle scan is an intelligent virus check that checks every file on your computer, regardless of whether or not it has previously been infected with a virus. The idle scan only ever works like a screensaver when you do not need your computer for a while, and immediately stops again as soon as you resume work, ensuring optimal performance for you. Here you can specify whether exception files or exception directories should be defined for the idle scan as well.

## Advanced

You can create additional virus scan settings by clicking the "Advanced" button.

In most cases, however, it is completely sufficient to use the specified default settings.

- **File types:** You can specify here which file types should be inspected by the software for viruses. Selecting the option "Program files and documents only" entails certain speed benefits.
- **Heuristics:** In the heuristic analysis, viruses are not only detected by the virus database, which you receive with every update of the antivirus software, but are also identified on the basis of particular characteristics typical of viruses. This method increases the level of security, but in rare cases may generate false alarms.
- **Check archive:** Checking compressed data in archives (these can be recognized by their file extensions such as ZIP, RAR or PST) is very time-consuming and can normally be omitted if the virus monitor is generally active on the system. To increase the speed of the virus check, you can limit the size of the archive files that are browsed to a specific value in kilobytes.
- **Check email archives:** Here you can specify whether your email archive is examined for infections as well.
- **Check system areas:** In general, system areas (e.g. boot sectors) in your computer should not be excluded from virus checks.
- **Check for diallers/spyware/adware/riskware:** You can also check your system for dialers and other malicious programs with this function. These are e.g. programs that establish expensive, unwanted Internet connections, in which the potential for financial damage is no less significant than that of a virus. They may for example secretly record your surfing habits or even all the keyboard entries you make (including your passwords) and forward these to third parties via the Internet at the earliest opportunity.
- **Check for rootkits:** Rootkits attempt to evade conventional virus detection methods. Additional monitoring for this malware is always advisable.

- **Only check new or modified files:** If you activate this function, files that have not been changed for a long time and that were previously flagged as harmless are skipped. This provides a performance improvement in everyday work – without compromising security.
- **Generate log:** You can use this checkbox to require the software to set up a log for the virus check process. This log can be viewed in the Logs area.
- **Offer virus checking for removable data media:** If you check this box, whenever a removable data medium (USB stick, external hard drive etc) is connected to your computer, you will be asked whether the device should be checked for viruses.

## Updates

If updating the software or virus signatures via the Internet does not work, you can perform all the operations necessary to enable updates to take place automatically in this area. In the options, enter the access data (user name and password) that you received via email when you registered your software online. The G DATA update server will use this data to recognize you so updates can now run completely automatically.

If you have purchased a new license and want to activate it, select [Activate licence](#). The [Internet settings](#) display special options that are only required in a few exceptional cases (proxy server, other region). The version check should only be temporarily disabled if you are having difficulty updating the virus signatures.

**Manage access:** With this option you have the chance of defining for yourself which Internet connections you want use for receiving software updates. This is especially useful if you sometimes connect via a network in which data transfers are paid for, e.g. with specific mobile phone tariffs with no real data flat rate.

**Virus signature import/export:** With computers that are never or only rarely connected to the Internet, or where there are restrictions on the data volume for downloads, you can also update virus signatures via a data medium (e.g. USB stick), or run an **offline update**. To do so, you must export the virus signatures to the storage medium using a computer that is connected to the Internet and has the necessary permissions. You can then import them via the "Import from" function on the computer with no Internet connection. The system on this computer will then be protected by the latest virus signatures as well. Unlike regular virus updates via the Internet, here this is up to the user, who must ensure him- or herself that signature updates are run as often as possible.

## Automatically update virus signatures

If you do not want the G DATA software to bother automatically updating the virus signatures, you can remove the check here. However, disabling this entails a high security risk and should only be done in exceptional cases. If the period between updates is too short for you, you can adjust it as you want and e.g. specify that updates should only be carried out when connecting to the Internet. This option is useful for example with computers that are not permanently connected to the Internet.

**Generate log:** If you check this box, every virus signature update is recorded in the log, which you can view in the additional G DATA software functions (in [SecurityCenter](#) under [Logs](#)). Besides these entries, you will find e.g. information on virus detections and other actions carried out by the software in the log.

## Activate licence

If you have not yet registered your G DATA software, you can do this now by entering your registration number and customer data. Depending on the type of product, you will find your registration number e.g. on the back of the user manual, in the confirmation email for a software download, or on the CD sleeve. On entering the registration number your product will be enabled.

Click the **Login** button and your access data will be generated on the update server. If the login is successful, an info screen appears with the message **Logged in successfully**, which you can exit using the Close button.

**Warning:** You will also receive access data for your documentation and for any software reinstallations by email. Therefore please make sure that the email address indicated in your online registration is correct; otherwise you will not receive the access data.

Finally the access data is automatically transferred to the original input mask so you can now update virus signatures via the Internet.

**Unable to activate your license?** If you cannot log in to the server, this may be due to a proxy server. Click on the [Internet settings](#) button. You can then check the settings for your Internet connection. If there are problems updating the virus signatures, by default you should first check whether you can access the Internet from a web browser (e.g. Internet Explorer). If you cannot connect to the Internet at all, the problem probably lies with your Internet connection and not with the proxy server data.

## Internet settings

If you use a proxy server, please put a checkmark next to **Use proxy server**. You should only change these settings if your virus signature update is not working. If necessary, consult your system administrator or Internet service provider about the proxy address. If necessary you can also enter the access data for the proxy server here.

**Proxy server:** A proxy server consolidates all requests to networks and distributes them to computers connected to it. If for example you use your computer in a company network, it may be useful for you to connect to the net via a proxy server. In the event of problems with the virus signature update you should generally first check to see if you can access the Internet at all via a web browser. If you cannot connect to the Internet at all, the problem probably lies with your Internet connection and not with the proxy server data.

## Web protection

If web protection is enabled, web content is checked for malware while you are browsing. You can create the following settings here.

- **Scan web content (HTTP):** Under the web protection options you can specify that all HTTP web content should be checked for viruses, even when browsing. Infected web content is not run at all and the corresponding pages are not displayed. To set this option, please check **Scan web content (HTTP)**.

If you do not want to check web content, the virus monitor will still of course take action if infected files are executed. That means your system is also protected without checking Internet content as long as the virus monitor is active.

You can also specify certain websites as exceptions if you consider them harmless. For more information please read the section [Define exceptions](#). You can use the [Advanced](#) button to create further settings for handling web content.

- **Phishing protection:** With so-called phishing, scammers on the Internet attempt to redirect customers of a particular bank or shop to fake websites in order to steal their data there. Activating the phishing protection is highly recommended.
- **Submit URLs of infected websites** Through this function you can automatically – and anonymously of course – report websites that are deemed unsafe by the software. With that, you optimise security for all users.
- **BankGuard browser protection:** Banking Trojans are becoming more and more of a threat. Every hour, online criminals are developing new malware variants (like ZeuS or SpyEye) that they use to steal your money. Banks secure data traffic on the Internet. However, the data is decrypted in the browser and banking Trojans can attack it there. However, the pioneering BankGuard technology from G DATA secures your banking transactions from the outset and provides instant protection where the attack takes place. By checking that the network libraries used are genuine, G DATA BankGuard ensures that your web browser has not been manipulated by a banking Trojan. We recommend leaving G DATA BankGuard protection switched on.

Note: Besides the man-in-the-middle method, in which the attacker manipulates the communication between the user and the target computer, there is also the man-in-the-browser (MITB) attack method. With this method, the attacker infects the browser itself and accesses the data before it is encrypted. The BankGuard module also protects you against this type of attack, by comparing the so-called digital fingerprint of a file or a part of a web page with a database on the Internet. In this way fraud is immediately detected and the G DATA software automatically converts the fraudulent data connection back to the original.

- **Keylogger protection:** Keylogger protection also monitors whether keyboard input on your system is being spied on, independently of virus signatures. This would give attackers the option of logging your password input. This function should always be enabled.

## Define exceptions

To add a website to the exceptions in the whitelist, please proceed as follows:

- 1 Click on the **Define exceptions** button. The Whitelist window will appear. This will display the websites that have been categorised as safe and entered here.
- 2 To add another website, please click on the **New** button. An input screen will appear. Enter the name of the website (e.g. [www.harmlessite.com](http://www.harmlessite.com)) under **URL** and, if necessary, enter a comment under **Note** about why you have included this website. Confirm your input by clicking on **OK**.
- 3 Now click on **OK** to confirm all changes to the whitelist.

To remove a website from the Whitelist, highlight it in the list using your mouse and then just click on the **Delete** button.



## Advanced

Here you can specify which server port numbers should be monitored by web protection. Generally port number 80 will suffice for monitoring normal browsing.

- **Avoid browser timeout:** Since the software processes web content before it is displayed in the web browser, it requires a certain amount of time to do so depending on the data traffic. Therefore it is possible for an error message to appear in the web browser because the browser is not receiving data immediately, since the antivirus software is checking it for malicious routines. By activating the **Avoid browser timeout** checkbox, you can disable this error message and, as soon as all browser data has been checked for viruses, the data will appear as normal in the web browser.
- **Enable notification when checking downloads:** Enable this function to get a notification whenever a download is being checked.
- **Size limit for downloads:** You can use this function to interrupt HTTP checks for web content that is too large. The contents are then monitored by the virus monitor as soon as suspected malicious routines become active. The advantage of the size limit is that there are no delays caused by virus checks when surfing the web.

## Email check

The email check enables you to scan incoming and outgoing emails and file attachments for viruses and eliminate possible infections at the source. The software can directly delete file attachments or repair infected files if viruses are found.

**Warning:** In Microsoft Outlook, emails are scanned by a plugin. This provides the same level of protection as the protection function for POP3/IMAP offered by AntiVirus. After installing this plugin, you will find the **Scan folder for viruses** function in the **Extras** Outlook menu, which you can use to check your mail folders individually for virus contamination.

## Incoming mail

The following options are available for virus protection for incoming emails:

- **In case of an infection:** Here you can specify what is supposed to happen if an infected email is discovered. Depending on the purposes for which you are using your computer, different settings apply here. Generally we recommend using the **Disinfect (if not possible: delete attachment/text)** setting.
- **Check incoming email:** By activating this option, all emails you receive while you are working on your computer are checked for viruses.
- **Append report to received, infected mails:** When you enable the report option and a virus is found, the warning **VIRUS** appears in the subject header of the infected email. There is also a message at the beginning of the email text: **Warning! This email contains the following virus** followed by the virus name and whether the virus has been deleted or whether it was possible to repair the infected file.

## Outgoing mails

The software also allows you to scan your emails for virus infection before you send them, to ensure you do not inadvertently send viruses yourself. If you try to actually send a virus (unintentionally), the message **The email [subject header] contains the following virus: [virus name]** appears. The mail cannot be sent, and the corresponding email will not be sent. Please check the box next to **Check emails before sending** to scan outgoing emails.

## Scan options

Here you can enable or disable basic virus check options:

- **Use engines:** The software works using two engines – two analysis units optimized for one another. In principle, use of both engines should guarantee optimum virus protection results.
- **OutbreakShield:** This option lets you activate the OutbreakShield. With OutbreakShield activated, the software creates checksums of emails, compares these with constantly updated anti-spam blacklists on the Internet and, as a result, is able to react to a mass-mailing before the relevant virus signatures become available. OutbreakShield uses the Internet to monitor increased volumes of suspicious emails, enabling it to close the window between the mass mail outbreak and its containment with specially adapted virus signatures, practically in real time. The OutbreakShield is an integral part of the email virus blocker.

## Encrypted connections (SSL)

Many email providers (such as GMX, WEB.DE, T-Online and Freenet) have now started using SSL encryption. This means that emails and email accounts have become significantly more secure. However, it is still necessary to use antivirus software to protect your email as well. G DATA offers the **Encrypted Connections module (SSL)** for this. This gives you the added option of checking SSL-encrypted email for viruses and malware.

To enable the G DATA software to check email that has been SSL-encrypted, a G DATA software certificate must be imported into the email program. This ensures that your G DATA software can check incoming email.

It supports all email programs that can either import certificates or can access the Windows certificate store, e.g.:

- Outlook 2003 or higher
- Thunderbird
- The Bat
- Pegasusmail

Please proceed as follows if the G DATA certificate is not installed automatically:

1. Your email program should not be active when installing the certificate. Therefore please close all email programs before generating and installing the certificate.
2. In the G DATA software, check the box next to Check SSL Connections.
3. Click on the Export Certificate button. The G DATA software will now generate a certificate. This file is called GDataRootCertificate.crt.
4. Now open the GDataRootCertificate.crt file. A dialogue window appears in which you can install the certificate on your computer.
5. In the dialogue window, click on the **Install Certificate** button and follow the instructions from the installation wizard.

You are done. Outlook and every other email program that can access the Windows certificate store now has the certificate required for checking SSL-encrypted incoming email for viruses and other malware.

**Note:** If you use **Thunderbird (portable)** and the certificate is not imported automatically, you will need to import this later and manage the trust settings for the generated G DATA certificate. To do this, please select the **Certificates** button in Thunderbird (portable) under **Options > Advanced > Certificates**. If you click here, various tabs appear. Please select the **Authorities** tab and then the **Import** button. You can now select the "**G DATA Mail Scanner Root**" certificate.

If you now check the boxes next to the following option fields and click OK, your Thunderbird portable will be protected by G DATA:

- **Trust this CA to identify websites.**
- **Trust this CA to identify email users.**
- **Trust this CA to identify software developers.**

There are similar functions in other email programs for importing certificates. In case of doubt, please see the appropriate help text to read how this works for the email program you use.

## Advanced

If you do not use the default ports for your email programs, you can enter the port you use for incoming or outgoing emails under **Server port number**. Click on the **Default** button to automatically restore the default port numbers. You can also enter multiple ports. Separate each of these with a comma.

**Warning:** Microsoft Outlook is protected by a special plugin that allows you to scan folders and emails directly from Outlook. In order to scan an email or a folder in Outlook for viruses, just click on the G DATA icon and the currently selected email folder will be scanned.

Since the software processes incoming emails before the email program itself, you may get an error message if there is a large quantity of emails or the connection is slow. This is because it is not receiving the email data immediately as it is being scanned for viruses by the software. Such error messages in the email program are prevented by checking the box next to **Avoid mail server timeout**, and as soon as any email data has been scanned for viruses, it is then forwarded to the email program as normal.

# Automatic virus checks

You can switch the idle scan on or off from here. Furthermore you can also regularly scan your computer, or areas of your computer, for infections instead or as well. For example, you can then run such scans at times when you are not using your computer.

**Scheduled virus checks:** In many cases it is sufficient for the computer to be checked by the idle scan. However, you can also use the **New** button to set up various automatic virus checks that are independent of one another. Hence it is possible for you to check the Downloads folder daily, whereas you check your MP3 collection only once a month for example.

The following sections explain how you set up individual virus checks.

## General

Enter the name you want to give the newly created virus check here. It is a good idea to use meaningful names to differentiate between the various jobs, for instance, *Local hard disks (weekly scan)* or *Archive (monthly scan)*.

If you check **Switch off the computer after completion of job**, the computer will automatically shut down once the automatic virus check has been completed. This is useful if for example you want to run a virus check when your day at work has finished.

**Job:** Each individually listed, automatic task for checking the computer or specific areas of it is called a job.

## Analysis scope

Here you can choose whether the virus check should be done on the local hard drives, whether memory and autostart areas should be tested, or if you only want to test certain directories and files. If this is the case, use the **Selection** button to specify the directories you want.

**Select directories/files:** In the directory tree, you can open and select directories by clicking on the plus symbols. Their contents will then be shown in the file view. Each directory or file that you mark with a check will be scanned by the software. If not all files in a directory are checked, this directory is marked with a grey checkmark.

## Scheduling

This 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 it in more detail under **Time**. Of course, if you select **On system start-up**, you need not set any scheduling as the software will run the scan each time your computer starts up.

- **Run job later if a client is not powered up at the scheduled time:** Activating this option means that virus checks that are not run automatically are automatically run later as soon as the computer is powered up again.
- **Do not run when in battery mode:** To prevent limiting battery service life unnecessarily, you can specify for notebooks, for example, that automatic virus checks can only be run when the portable computer is connected to the mains.

## Scan settings

This area allows you to define which settings should be used for the automatic virus check.

- **Use engines:** The software works with two engines – two virus checking programs optimized for one another. You can accelerate the virus check in older and slower computers by using just one engine, but normally you should keep the setting **Both engines**.
- **Infected files:** Has your software detected a virus? In the standard setting, the software now asks you what you would like to do with the infected file. If you would always like to perform the same action, you can set this here. The highest protection for your data is offered here by the setting **Disinfect (if not possible: place in quarantine)**.
- **Infected archive:** Here you determine whether archive files (e.g. files with the extension RAR, ZIP or PST) should be handled differently from normal files. However, please note that moving an archive to quarantine can damage it so that it can no longer be used after it is moved back.

Furthermore, you can click the button **Advanced** to specify which additional virus checks should be performed or omitted.

In most cases, however, it is completely sufficient to use the specified default settings.

- **File types:** You can specify here which file types should be inspected by the software for viruses.
- **Heuristics:** In the heuristic analysis, viruses are not only detected by the virus database, which you receive with every update of the

software, but are also identified on the basis of particular characteristics typical of viruses. This method increases the level of security, but in rare cases may generate false alarms.

- **Check archive:** Checking compressed data in archives (these can be recognized by their file extensions such as ZIP, RAR or PST) is very time-consuming and can normally be omitted if the virus monitor is generally active on the system. The monitor can detect a previously hidden virus while the archive is being unzipped and can automatically prevent it from spreading.
- **Check email archives:** Here you can specify whether your email archive is examined for infections as well.
- **Check system areas:** In general, system areas (e.g. boot sectors) in your computer should not be excluded from virus checks.
- **Check for diallers / spyware / adware / riskware:** You can also use this function to check your system for diallers and other malware (spyware, adware and riskware). These are e.g. programs that establish expensive, unwanted Internet connections, of which the potential for financial damage is no less significant than that of the virus. They may for example secretly record your surfing habits or even all the keyboard entries you make (including your passwords) and forward these to third parties via the Internet at the earliest opportunity.
- **Check for rootkits:** Rootkits attempt to evade conventional virus detection methods. Additional monitoring for this malware is always advisable.
- **Generate log:** By checking this box, you can specify that the software creates a log of the virus check process. This log can be viewed in the **Logs** area.

## User account

Here you can specify the user account on the computer on which the virus check should take place. This account is required for access to network drives.

## AntiSpam

### 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. You can use the **Use spam filter** button to enable or disable the spam filter.

In order to switch the different filter types of the spam filter on or off, simply set or remove the checkmark in front of the respective entry. To make changes to the various filters, just click on the relevant entry. A dialog then appears for changing the parameters. The following settings options are available:

- **Spam 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 mail outbreak and its containment with specially adapted virus signatures, practically in real time. If you use a computer downstream from a proxy server, click on the **Internet settings** button to carry out the relevant changes. You should change these settings only if your OutbreakShield doesn't function.
- **Use whitelist:** Certain sender addresses or domains can be explicitly excluded from suspected spam via the whitelist. Simply enter the email address (e.g. **newsletter@infosite.com**) or domain (e.g. *infosite.com*) that you want to exclude from suspected spam in the *Addresses/Domains* field and the G DATA software will treat messages from that sender or sender domain as not 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.

- **Use 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 check for spam in the *Addresses/Domains* field and the G DATA software will generally treat emails from that sender or sender domain as emails with a 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.
- **Use real-time blacklists (default setting):** You can find lists on the Internet that contain the IP addresses of servers known to send spam. The G DATA software uses queries to the 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 settings here, although you can also

add your own Internet addresses to blacklists 1, 2 and 3.

- **Use 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 how you want 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 a list of keywords as a text file. By checking **Search for whole words only**, you can specify that the G DATA software will only search for complete words in the subject line of an email.
- **Use keywords (subject):** You can also identify suspected spam messages through the text 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 spam probability.
- **Use content filter:** The content filter is a self-learning filter that calculates spam probability on the basis of the words used in the email text. 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 words in this table by using the **Reset tables** button, after which the content filter will restart its learning process again from the beginning.

## Reaction

Here you can define how the spam filter should process email messages that may contain spam. You can use the spam probability value calculated for the affected email by the G DATA software to define three different levels of filtering.

- **Suspected spam:** Here you can define how those email messages in which the G DATA software finds individual spam elements are handled. Such messages may not generally be spam, but can also be newsletters or part of a mass mailing that is of interest to the recipient in rare cases. In such cases, it is recommended that you inform the recipient that the email is suspected spam.
- **High spam probability:** This covers emails that contain many spam characteristics and are rarely of interest to the recipient.
- **Very high spam probability:** These are emails that meet all the criteria of spam. Such emails are rarely wanted, and rejecting email with these characteristics is recommended in most cases.

Each of these three graduated reactions can be customised. Simply click on the **Change** button and define the response that the G DATA software should use. The **Reject email** option allows you to specify that the email messages do not reach your mailbox. And with **Insert spam warning in mail subject and mail text** you can call attention to email messages that have been identified as spam to enable these to be filtered more easily. If you use **Microsoft Outlook** (caution: not to be confused with Outlook Express or Windows Mail), you also have the option of moving emails containing suspected spam to a fully customizable folder in your mailbox (**Move mail to folder**). You can create this folder directly via the G DATA software by defining the corresponding folder under **Folder name**.

**Note:** Even if you do not use Outlook, email messages that have been identified as spam can be moved to a different folder. Just add an alert in the subject line of the message (for instance "[Spam]") and define a rule in your email program to move emails with this text in the subject line to a different folder.

## Advanced settings

This area enables you to make detailed changes to the G DATA software spam detection, adapting the system to suit your email traffic. However, it is generally recommended that default settings are used here. Making changes in the advanced settings should only be done if you have the relevant expertise and know exactly what you are doing.

## More filters

The following filters are created by default; however, if necessary you can also switch them off by unchecking the box.

- **Disable HTML scripts**
- **Filter malicious attachments**

You can use the **New** button to set up new filter rules, or edit existing filters with the **Edit** button. The filters created are shown in the list and can be enabled or disabled as required by checking the checkbox to the left. 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. To permanently delete a filter, click the relevant filter once to highlight it and then click the **Delete** button.

The filter options available here are additional filters that support the actual G DATA software spam filter and make it easier for you to configure your own personal settings. The spam filter provides you with an extensive range of setting options for effectively blocking

emails 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.

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.

- **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. In this event, scripts have the option of running not only when the infected attachment is opened but even in email preview mode.
- **Filter harmful attachments:** A large number of filter options for filtering email attachments are provided. Most email viruses are spread through attachments, which usually have more or less well-hidden executable files. This can be a standard .exe file containing malware, or a VB script hidden in a graphic, film or music file that is assumed to be safe. 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 extensions to which you would like to apply the respective filter. You can, for instance, combine all executable files (such as EXE and COM files) in a single filter, while also filtering out other formats (for instance MPEG, AVI, MP3, JPEG, JPG, GIF etc.) that are a burden for your mail server due to their size. You can, of course, also filter out archive files of your choice, such as ZIP, RAR or CAB files. Please use a semicolon to separate all file extensions of a filter group.

The function **Also filter attachments in embedded mails** 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 generally be enabled.

Choosing **Only rename attachments** has the effect that attachments that are to be filtered are not deleted automatically rather just 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 that should be appended to the file extension (\*.exe\_danger, for instance), which prevents this type of file from being executed by just clicking on it. 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 messages which contain certain subjects or text.

Simply enter the keywords and expressions to which the G DATA software should react under **Search criterion**. It is possible to use the AND and OR logical operators to link text components with one another.

Under **Search scope** you can now enter those elements of an email message that the software should search for the defined terms. The **header** is the part of an email message that, among other things, contains the email address of the sender and the recipient, the subject line, information on the programs and protocols used, and the date sent. If you have, for instance, activated **Subject** as the search area, only the content of the subject line will be checked, and no other information contained in the header. If you select **Mail text** as the search scope, you have the additional option of limiting the search scope to pure text emails, or extending the search to text in HTML emails (HTML text).

By checking **Embedded mails** you can define whether the content filter search should also cover email messages included as attachments in received messages.

Under **Reaction** you can determine what is to be done with emails identified as spam by the G DATA software. Using **Reject mail** means the email in question will not even be accepted by your email program.

If you check the box for **Insert warning in mail subject and text** you can prefix the actual text in the subject line with a warning (prefix in subject line), e.g. *Spam* or *Warning*. You can also enter text to be placed above the actual email text in the event of suspected spam (Message in text).

If you use *Microsoft Outlook* (**caution:** not to be confused with Outlook Express or Outlook Mail), you also have the option of moving emails containing suspected spam to a fully customizable folder in your mailbox (**Move mail to folder**). You can create this folder directly via the G DATA software by defining the corresponding folder under **Folder name**.

- **Sender filter:** You can use the sender filter to easily block email coming from certain senders. To do this, simply enter the email addresses or domain names to which the G DATA software should react under **Sender/domains**. Use a semicolon to separate multiple entries.

Under **Reaction** you can determine what is to be done with emails identified as spam by the G DATA software.

Using **Reject mail** means the email in question will not even be accepted by your email program.

If you check the box for **Insert warning in mail subject and text** you can prefix the actual text in the subject line with a warning (prefix in subject line), e.g. *Spam* or *Warning*. You can also enter text to be placed above the actual email text in the event of suspected spam (Message in text).

If you use *Microsoft Outlook* (**caution**: not to be confused with Outlook Express or Windows Mail), you also have the option of moving emails containing suspected spam to a fully customizable folder in your mailbox (**Move mail to folder**). You can create this folder directly via the G DATA software by defining the corresponding folder under **Folder name**.

- **Language filter**: The language filter lets you automatically define email in specific languages as spam. For example, if in general you do not 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 the G DATA software will raise the spam probability for such emails.

Under **Reaction** you can determine what is to be done with emails identified as spam by the G DATA software.

Using **Reject mail** means the email in question will not even be accepted by your email program.

If you check the box for **Insert warning in mail subject and text** you can prefix the actual text in the subject line with a warning (prefix in subject line), e.g. *Spam* or *Warning*. You can also enter text to be placed above the actual email text in the event of suspected spam (Message in text).

If you use *Microsoft Outlook* (**caution**: not to be confused with Outlook Express or Windows Mail), you also have the option of moving emails containing suspected spam to a fully customizable folder in your mailbox (**Move mail to folder**). You can create this folder directly via the G DATA software by defining the corresponding folder under **Folder name**.

## Miscellaneous

You can create more settings in this area.

- **Scan unread emails in the inbox at program start**: *Only for Microsoft Outlook*: This option is used for checking email for suspected spam. The G DATA software will then check all unread emails in your Inbox folder and subfolders as soon as you open Outlook.
- **Other email programs (using POP3)**: For technical reasons, emails received via POP3 cannot be deleted directly. If a filter is set to reject emails, this email is then assigned default replacement text. The replacement text for rejected email is: **The message has been rejected**. However, you can also customise the text for these notification functions. 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:

%s    *Sender*

%u    *Subject*

In your email client, you can define a rule that automatically deletes emails containing the replacement text defined here.

## Firewall

### Automatic

If you no longer want to deal with the firewall, you should switch the setting to Automatic. Besides autopilot mode, which is the best option for many users, you also have a wide range of options for optimizing the G DATA firewall for your requirements.

In the firewall settings there are two basic areas that can be custom-configured.

### Autopilot

Here you can specify whether the firewall should operate independently and in self-learning mode so the user is not consulted about deciding whether to block or allow queries from the Internet, or whether the user should be asked in case of doubt.

- **Autopilot mode**: Here the firewall works fully autonomously and automatically keeps threats from the local PC. This setting offers practical all-around protection and is recommended in most cases.
- **Create rules manually**: If you want to custom configure your firewall, you can set up your firewall protection how you want via manual rule creation.

- **Offer autopilot mode when a full screen application is launched:** During computer games (and other full-screen applications), it can be disruptive if the firewall interrupts the flow of the game with enquiry windows or simply interferes with the display. To ensure that you can enjoy uninterrupted gaming without security compromises, the autopilot is a useful setting because it suppresses the inquiries of the firewall. If you are not using the autopilot as a default setting, you can use this function to ensure that it is always activated if you are using a program running in full-screen mode.

## User-defined security settings

As you use the computer for your normal daily tasks, the firewall learns which programs you do or do not use for Internet access and which programs represent a security risk. The advantage of using the default security levels is that you can still adapt the firewall to your individual requirements without too much administrative input or specialist knowledge of network security. You can set the security level by simply adjusting the slide control. The following security levels are available:

- **Maximum security:** The firewall rules are generated using very strict guidelines. So you should be familiar with specialised network concepts (TCP, UDP, ports, etc.). The firewall detects the slightest inconsistencies and will issue frequent queries during the learning phase.
- **High security:** The firewall rules are generated using very strict guidelines. So you should be familiar with specialised network concepts (TCP, UDP, ports, etc.). The firewall may issue frequent queries during the learning phase.
- **Standard security:** The firewall rules are generated at the application level only. Wizards keep network-specific details away from you. You will be queried as little as possible during the learning phase.
- **Low security:** The firewall rules are generated at the application level only. Wizards keep network-specific details away from you. You will only be rarely queried during the learning phase. This level of security still offers highly effective protection against any connection requests that may occur.
- **Firewall disabled:** You can disable the firewall completely if required. This means that your computer is still connected to the Internet and any other networks, but the firewall is no longer protecting it against attacks or electronic espionage.

If you wish to create specific settings for your firewall, check **User-defined security settings**. Please note however that for these settings you'll need at least a basic understanding of network security.

## Queries

Here you can specify whether, when and how the firewall should query users when programs request a connection to the Internet or network.

### Define rule

If the firewall detects a connection being made to the network, an information box appears in which you specify how to proceed for this particular application. Specify here precisely how to proceed in terms of allowing or forbidding network access:

- **Per Application:** This enables you to specify universal authorization or denial of network access by the currently selected application on any port and using any transfer protocol (e.g. TCP or UDP).
- **Per Protocol/Port/Application:** The application requesting network access is only permitted to go online with the requested transfer protocol and on the specified port. If the same application requests an additional network connection on another port or using a different protocol, the query will appear again, allowing you to create another rule for it.
- **Application, if at least x inquiries are pending:** There are applications (e.g. Microsoft Outlook) that send identical requests to multiple ports when requesting network access or that use different protocols simultaneously. Since, for example, this would cause several queries in the Protocol/Port/Application setting, you can specify here that applications should receive general permission or refusal for network use as soon as you have allowed or denied connection by the user.

### Unknown server applications

Applications that are not yet managed using a rule in the firewall may be handled in a different manner. The time of the inquiry lies within a certain latitude. If the server application goes to "on receipt", this means that it is waiting for a connection request as if on standby. Otherwise the query is only generated when the actual connection request is made.

### Check for unprotected networks

Of course, a firewall can only function properly if all the networks accessed by the computer it is protecting can also be detected and monitored by it. Therefore you should always have this check enabled for unprotected networks.



## Repeat application queries

You can bundle recurring requests for connection of an application. This way, queries do not keep appearing during connection attempts for which you have not yet specified a rule, but rather only in e.g. 20-second intervals or some other period of time defined by you.

## Reference testing

During reference checking the firewall calculates a checksum based on the file size and other criteria for applications for which it has already enabled network access. If the checksum for this program suddenly changes, it may be because the program has been modified by a malware program. In such cases, the firewall generates an alarm.

**Perform reference checking for loaded modules:** Here not just applications but also modules used by applications (e.g. DLLs) are monitored. Since these frequently change or new modules are downloaded, consistent checking for modified and unknown references for modules may result in a considerable administration effort. Every modified module would cause a security request to be sent in its trail to the firewall. Therefore module checking should only be used in this way for very high security requirements.

## Miscellaneous

Further setting alternatives are available here.

### Wizard default settings

Specify here whether, in general, you wish to create new rules using the Rule wizard or in advanced editing mode. For users who are not familiar with the subject of network security, we recommend using the rule wizard.

### Check a program at startup

Here you can specify whether the firewall looks for unknown server applications on each program startup. These search functions should always be enabled unless you are working in an enclosed network.

### Save connection log



Here you can specify for how long the firewall connection data should be saved. You can retain the data for anywhere between an hour and 60 hours and view it in the Log area.

## Tuner

### General

You can create the following settings here:

- **Delete restore data:** Here you can specify when restore data (which the G DATA software creates in the event of changes) should be deleted.
- **Delete old data:** Here you can specify when old data (e.g. old TEMP folders) should be deleted.
- **Delete desktop shortcuts:** Here you can specify when desktop shortcuts that are not required (that have not been used for a corresponding number of days) should be deleted.
- **Search for Office updates as well during Microsoft updates:** Here you can specify whether or not the tuner is supposed to search the Internet automatically for current Windows updates and Office updates. Updating both elements saves time and keeps you fully up to date from a security technology perspective. Of course, the search for Office updates only works if Microsoft Office is installed on the relevant computer.
- **Do not create detailed logs about deleted items:** The tuner is structured in such a way that it consistently logs information about any changes that are made. If you think that a log file containing relevant information on what the tuner has deleted is a security risk, you can suppress the creation of such a deletion log.
- **Permanently delete temporary files:** You can use this function to exclude web files (e.g. cookies, temporary Internet files etc.) from the tuner's restore option, i.e. you can prevent such files from being restored. By activating this function, you considerably reduce the number of files that the tuner has to manage in the Restore area. This improves performance.
- **Automatic computer restart not permitted by the service:** You can use this option to prevent a possible computer restart that the tuner might otherwise carry out as part of a scheduled tuning process. Since the tuner would only perform a computer restart

without asking when no user is logged on, it is definitely recommended that this option is not activated in the majority of cases.

- **Allow creation of individual restore points:** Without this function the G DATA software can no longer carry out a restore.
- **Ignore volume type when defragmenting:** As the majority of vendors recommend against defragmenting their SSDs, defragmenting is excluded in the G DATA Tuner for this type of drive by default. If the type of the G DATA software drives cannot be automatically determined, but you are certain that there are no SSD volumes in your computer, you can leave the box here checked. The tuner will then start defragmenting every hard drive located in the system every time it is run.

## Configuration

In this area you can select all the modules that the tuner should use for a tuning process. Selected modules are then either started automatically as a scheduled event (see [Scheduling](#)) or manually. To activate a module simply double-click it. You can optimise the following main tuning areas as you want here:

- *Security:* Various functions that download data automatically from the Internet are only of use to the provider and have no benefit for you. These functions may often leave you vulnerable to malware. With these modules you can protect your system and keep it up-to-date.
- *Performance:* Temporary files, e.g. backup files that are no longer required, log files or installation files that still take up disk space following the installation slow down your hard drive and take up valuable disk space. Moreover processes and file links that are no longer required can significantly slow down your system. You can use the modules listed here to remove this superfluous load from your computer and speed the computer up.
- *Data protection:* This summarises the modules that deal with protecting your data. Traces that are created unintentionally while surfing or using the computer in general and that contain a lot of information about your user behaviour, or even important data and passwords, are deleted here.

## Folder protection

On this tab you can exclude specific folders (including your Windows partition) from being automatically deleted with old files.



Just click the **Add** icon and select the corresponding folder or the desired drive.



To grant access to excluded folders again, select them from the displayed list and click on the **Delete** button.

## File protection

You can use file protection to protect certain files from being deleted by the tuner, for example game scores for computer games or similar files with unusual file extensions, which could also be interpreted as backup or temp files.



To protect specific files, click the **Add** button and enter the corresponding file name. You can also use wildcards here.

Wildcards function as follows:

- The question mark symbol (?) represents individual characters.
- The asterisk symbol (\*) represents entire character strings.

For instance, in order to protect all files with the file extension .sav, enter \*.sav. To protect e.g. files of different types that have file names that start identically, you enter text\*.\* for example.

Now choose the folder in which the files are to be protected by clicking the Advanced button. Here you can now select the storage location where the files to be protected are located. The Tuner now protects the files thus defined in this folder only (e.g. only game scores in the relevant games folder).



To grant access to excluded folders again, select them from the displayed list and click on the **Delete** button.

# Scheduling

The **Scheduling** tab allows you to specify when the automatic tuning job should run and how often.

Under **Daily**, you can use the Weekdays settings, for example, to specify that the computer should only carry out the tuning job on workdays or just every other day, or on weekends only, when it is not being used for work. To change date and time entries under **Time**, simply highlight the element you want to change (e.g. day, hour, month, year) with the mouse and use the arrow keys or the small arrow icon to the right of the input field to move the relevant element chronologically.

If you do not want to run an automatic tuning process, just remove the check from the box next to the **Enabled** entry for the automatic tuning process.

# Device control

You can use device control to specify for your computer which storage media are permitted to read and/or write data. Hence for example you can prevent private data from being moved to a USB stick or burned to a CD. Furthermore, with removable data carriers such as USB sticks or external USB hard drives, you can specify precisely which removable data carriers can be used for downloading data. This means for example that you can use your own USB hard drive to back up data, but other hard drives are not granted access.

To use device control, check the box next to **Enable device control** and select the devices you want to define restrictions for:

- **Data media (e.g., USB sticks)**
- **CD/DVD drives**
- **Disk drives**

You now have the option of defining rules for the individual storage media.

## General rules

Here you can specify whether the relevant device cannot be used at all (**Block access**), whether it can only download data but not be used for storing it (**Read access**), or whether there are no restrictions for this device (**Full access**). This rule then applies for all users of your computer.

## User-specific rules

If you want to grant restricted permissions for storage media to specific users only, in this area you can first select the user name of the user set up on your computer then restrict access to the relevant storage medium as described in **General rules**. In this way, for example, as administrator and owner of the computer you can permit full access for yourself but just restricted permissions for other users.

Select the user here. If you now click on OK, another dialog opens in which you can specify which access method you want for this user and whether authorization for this user is limited to a specific period (e.g. two weeks) (**Validity**).

**Note:** User-specific rules override general rules. This means that if you specify generally that access to USB sticks is not permitted, you can still allow a specific user to use them via a user-specific rule. If a user has been allocated certain access restrictions via device control that are time-limited, the general rules will apply for this user again when this restriction expires.

## Device-specific rules

When using removable data carriers such as USB sticks or external hard drives, you can also specify that only specific removable data carriers are allowed to access your computer. To do so, attach the removable data carrier to your computer and click on the **Add** button. In the dialog that appears, you can select the removable data carrier you want. If you now click on OK, another dialog opens in which you can specify which access method you want for this data carrier and whether authorization for this data carrier is limited to a specific period (e.g. two weeks) (**Validity**) and whether every user is allowed to use this data carrier under his user access or not.

# Backup

In this area you can create general settings for the backup module functionality.

- **Directory for temporary files:** Specify here where temporary backup module data should be saved. These files are created when generating or restoring a backup, and are automatically deleted again when the relevant process is complete. However, you need to have sufficient hard disk storage space available here, otherwise the backup/restore speed will be limited. This setting should only be changed if there is insufficient storage space available for temporary files on the selected drive.
- **Check source/destination drive on same hard disk:** Normally the backup module will warn the user whenever he tries to create a backup on the same data medium that the original files are located on. This occurs because, in the event of a failure or loss of this data medium, by default the backup would no longer be available either. However, if you want to regularly run backups to the original data medium for a specific reason, you can disable this warning message here.

# Logs

The individual modules have log functions that you can use to get an overview at any time of the actions that your G DATA software is carrying out to protect you.

## Virus protection logs

The log area lists the logs made by the software. Click the **Start time**, **Type**, **Titel**, or **Status** column headers to sort the available logs accordingly. The **Save as** and **Print** buttons can be used to save log data as text files or print them out directly. To delete a log, highlight the entry in the table using the mouse and either press the Del key or click on the **Delete** button.

## Firewall logs

The Logs area provides a comprehensive log file for every firewall action. Here you can open individual actions by double-clicking on them and print them out as required or save them as text files. For more information see the section entitled [Settings: Miscellaneous](#).

## Backup logs

The Logs area provides a comprehensive log file for every action and every backup job. Here you can open individual actions by double-clicking on them and print them out as required or save them as text files. For more information see the section entitled [Backup and restore](#).

## Spam protection logs

The Logs area provides a comprehensive log file for every action. Here you can open individual actions by double-clicking on them and print them out as required or save them as text files.

## Parental controls logs

In the log area, you as the administrator have an overview of all attempts made by other users to call up blocked content. For that purpose you have to select a user from the list at the top of the screen to display his/her specific log. Please also refer to the section [Settings: Log](#).

**Note:** You can, of course, also delete these logs using the **Delete logs** button.

## Device control logs

The Logs area provides a detailed log file of every device manager activity. You can also read about this in the following section: [Settings: Device control](#)

# FAQ: boot scan

If your computer is brand new, or has been protected by antivirus software until now, you can run the installation as follows.

However, if you have good reason to suspect that your computer has already been infected by a virus, it is recommended that you run a boot scan before installing the software.

**BootScan:** When you switch on your computer, your Windows operating system starts automatically as normal. This process is called booting. However, there is also the possibility of other operating systems and programs being launched automatically.

To scan your computer for viruses before Windows starts, G DATA provides you with a special bootable version in addition to the Windows version.

## Prerequisites

The BootScan helps you fend off viruses that have embedded themselves on your computer prior to installing antivirus software.

To do this, there is a special version of the software that can be run prior to starting Windows.

**Booting from CD/DVD-ROM:** If your computer will not boot from a CD/DVD-ROM, you can carry out the following procedure:

- 1** Switch your computer off.
- 2** Restart your computer. Usually you reach the BIOS setup by pressing the DEL button (or F2 or F10 as well depending on your system) as the computer boots up.
- 3** How to change individual settings in your BIOS setup varies from computer to computer.

To do this, please consult your computer's documentation.

This means that the boot sequence should be **CD/DVD-ROM, C**, i.e. the CD/DVD-ROM drive becomes the **1st boot device** and the hard drive partition with your Windows operating system is the **2nd boot device**.

- 4** Save the changes and restart your computer. Your computer is now ready for a boot scan.

**How do I cancel a boot scan?** If your computer displays the G DATA BootScan software interface instead of the usual Windows environment after restarting, there is no cause for concern.

If you have not planned to run a boot scan, just use the arrow keys to select the **Microsoft Windows** entry, then click **Return**. Windows will now start normally, without first carrying out a boot scan.

**Booting from USB stick:** If you use a USB stick as a boot medium, you can also select this as the 1st Boot Device.

# FAQ: Program functions

## Security icon

Your G DATA software will permanently protect your computer against viruses and malware. An icon appears in the taskbar at the bottom next to the clock, so you can see that the protection is active.



This G DATA icon tells you that everything is OK and that protection for your computer has been enabled.



If the monitor is disabled or some other problem occurs, the G DATA icon displays a warning message. You should then start the G DATA software as soon as possible and check the settings.

If you right-click the icon, a context menu appears which you can use to control the basic security functions of the software.

The following functions are available:

- **Start G DATA software:** This allows you to access the SecurityCenter where, for example, you can configure the virus monitor settings. Read about what you can do in the SecurityCenter in the section: [SecurityCenter](#)
- **Disable monitor:** You can use this to disable and also re-enable the virus monitor as required. This may be advisable if, for example, you are copying large volumes of data from one part of your hard drive to another or running memory-intensive processes (such as copying DVDs, etc.). You should only leave the virus monitor disabled when absolutely necessary and make sure, wherever possible, that your system is not connected to the Internet during this time and that it cannot access any new, unscanned data (e.g. from CDs, DVDs, memory cards or USB sticks).
- **Disable firewall:** If you use a version of the G DATA software with an integrated firewall, you can switch the firewall off via the context menu if necessary. This means that your computer is still connected to the Internet and any other networks, but the firewall is no longer protecting it against attacks or electronic espionage.
- **Disable autopilot:** The autopilot is a component of the firewall that decides independently which queries and contacts your computer needs to accept via the network and Internet. The autopilot is ideal for normal use and you should always have it enabled. Like the firewall, the autopilot is available in certain versions of the G DATA software.
- **Update virus signatures:** Antivirus software should always be fully up to date. You can of course have the data updated automatically by the software. However, if you urgently need an update, you can launch one via the **Update virus signatures** button. Read about the purpose of a virus update in the section: [Virus check](#)
- **Statistics:** Here you can view statistics on virus monitor checking processes, as well as find information on idle scans, web filter messages and other parameters.

## Run virus check

With the virus check, you check your computer for infestation by malware. If you start the virus check, it monitors every file on your computer as to whether it can infect other files or is itself already infected.

If viruses or other malware are found during a virus check, there are different options as to how the virus can be removed or disarmed.

- 1 Start the virus check. You can read how to do this in the section entitled: [Virus protection](#)
- 2 Now a check of your computer for virus infestation occurs. A window opens for this which includes information on the status of the check.

A progress bar at the top of the window tells you how far the system check has progressed. While the virus check is taking place you have a number of options for influencing the course of the virus check:

- **Pause the virus check at times of high system load:** You can use this option to specify that the software holds the virus check until you are finished with other tasks on your computer.
- **Switch off computer after virus check:** This function is very useful if you want to run the virus check overnight or at the end of the working day. As soon as the virus check by the G DATA software has completed, your computer will be powered down.
- **Password-protected archive:** As long as an archive is password-protected, the G DATA software cannot scan the files in it for



viruses. If you check this box, the antivirus software indicates which password-protected archives it was unable to scan. Provided the archives are not unpacked, any viruses it contains will not pose a security risk to your system.

- **Access denied:** In Windows, there are usually files that are used exclusively by applications and that can therefore not be scanned while these applications are running. It is preferable that you therefore have no other programs running on your system during a virus check. If you set a checkmark here, the data that is not checked will be displayed.

**3a** If your system is virus-free, you can exit the wizard window after the check has finished using the **Close** button. Your system has now been checked and cleared of viruses.

**3b** In the event that viruses and other malware are found, you can decide how to handle the virus discovery. Generally clicking on the **Execute actions** button is sufficient.

The G DATA software now uses a default setting (if no other settings have been made under [Settings: Manual virus check](#) for infected files and archives) and disinfects the affected files, i.e. it repairs them so they can be used again without restriction and are no longer a threat to your computer.

If such disinfection is not possible, the files are placed under quarantine, i.e. they are encrypted and moved to an extra safe folder where they cannot cause any further damage.

If you still need this infected file, in exceptional cases you can retrieve the file from quarantine and use it again.

Your system has now been checked and cleared of viruses.

**3c** If you are familiar with the infected files/objects and can tell which ones are no longer required, you also have the option of customising precisely how to respond to each virus discovery.

You can use the Action column in the list of virus discoveries to define what should happen with each individual infected file.

- **Log only:** The infection is listed in the [Logs](#) view. However, the files concerned are not repaired or deleted. **Warning:** If a virus is only logged, it continues to be active and dangerous.
- **Disinfect (if not possible: log only):** Here, an attempt is made to remove the virus from an affected file; if this is not possible without damaging the file, the virus is logged and you can deal with it later via the log entry. Warning: If a virus is only logged, it continues to be active and dangerous.
- **Disinfect (if not possible: place in quarantine):** This is the default setting. Here, an attempt is made to remove the virus from an affected file; if this is not possible without damaging the file, the file is moved to the [Quarantine](#). Please read about this in the section: [Quarantined files](#)
- **Disinfect (if not possible: delete file):** An attempt is made to remove the virus from a compromised file; if this is not possible, the file is deleted. This function should only be used if there is no important data on your computer. Always deleting infected files can, in the worst case, result in your Windows becoming inoperable and requiring a reinstallation.
- **Move file to quarantine:** Infected files are immediately moved to the Quarantine. Files saved in the quarantine are encrypted. The virus cannot cause any damage here, and the infected file is still available for possible repair attempts. Please read about this in the section: [Quarantined files](#)
- **Delete file:** This function should only be used if there is no important data on your computer. Always deleting infected files can, in the worst case, result in your Windows becoming inoperable and requiring a reinstallation.

If you click on the **Execute actions** button now, the G DATA software proceeds with each virus discovery as you have specified.

Your system has now been checked for viruses. However, if you have used a setting with the **Log** option, it may be that your computer is not virus-free.

## Virus alarm

If the G DATA software finds a virus or other malware on your computer, a message window appears at the edge of the screen.

You now have the following options for dealing with the infected file.

- **Log only:** The infection is listed in the Logs view. Repair or deletion of the affected file does not occur. However, you can individually check the detected viruses via the log and remove them in a targeted manner. Warning: If a virus is only logged, it continues to be active and dangerous.
- **Disinfect (if not possible: move to quarantine):** Here, an attempt is made to remove the virus from an affected file; if this is not possible without damaging the file, the file is moved to the Quarantine. Please read about this in the section: [How does the quarantine work?](#)
- **Move file to quarantine:** Infected files are immediately moved to the Quarantine. Files saved in the quarantine are encrypted. The virus cannot cause any damage here, and the infected file is still available for possible repair attempts. Please read about this in the section: [Quarantined files](#)
- **Delete infected file:** This function should only be used if there is no important data on your computer. Always deleting infected files can, in the worst case, result in your Windows becoming inoperable and requiring a reinstallation.

**Quarantine and mailboxes:** There are files where a move to quarantine is not recommended, e.g. the archive files for mailboxes. If a mailbox is moved to the quarantine, your mail program can no longer access it and may no longer work. Therefore you should be especially careful with *files with the extension PST*, since these usually contain the data from your Outlook mailbox.

## Firewall alarm

When in manual rule creation mode, the firewall will generally check unknown programs and processes that try to connect to the network, to see if this should be allowed or denied. An information box will open to show you details about the relevant application. You can also allow one-off or permanent access to the network, or deny any access. As soon as you have allowed permanent access to a program, or have denied access, a new rule will be created in that network's rule sets for this and you will not be asked about this again.

The following buttons are available:

- **Always permit:** Use this button to create a rule for the application indicated above (e.g. Opera.exe, Explorer.exe or iTunes.exe), granting it permanent access to the network or Internet on the network specified for the application. You will also find this rule as Rule created by enquiry in the area called Rule sets.
- **Permit this time:** You can use this button to permit the relevant application to access the network only once. The firewall will issue another alert the next time this program attempts to access the network.
- **Always block:** Use this button to create a rule for the application indicated above (e.g. dialer.exe, spam.exe or trojan.exe), permanently denying it access to the network or Internet on the network specified for the application. You will also find this rule as Rule created by enquiry in the area called Rule sets.
- **Block this time:** This button lets you deny the relevant application access to the network once only. The firewall will issue another alert the next time this program attempts to access the network.

There is further information available on the protocol, port and IP address with which the relevant application is trying to interact.

## Not a virus message

Files reported as "not a virus" are potentially dangerous applications. Such programs do not have malware directly but may be used against you by attackers under certain circumstances. This category can include certain tools for remote administration, programs for automatically switching the keyboard layout, IRC clients, FTP servers or different tools for creating or hiding processes.

## Uninstall

If you want to remove the G DATA software from your computer again at any point, please run the uninstall function via your operating system's control panel. The uninstall then takes place automatically.

If the G DATA quarantine folder still contains files at the time of uninstalling, you will be asked whether you wish to delete these files or not. If you do not delete the files, they remain encrypted on your computer in a special G DATA folder and are therefore incapable of causing any harm. You can only use these files again by reinstalling the G DATA software on your computer.

During the uninstall process, you will be prompted whether you want to delete the program settings and logs. If you do not delete these

files, the logs and settings will be available on reinstallation of the software.

Complete the uninstall process by clicking on the **Exit** button. The software is now completely uninstalled from your system.

# FAQ: License questions

## Multi-user licenses

You can use multi-user licenses to operate the G DATA software on the licensed number of computers. You will receive online access data after installation on the first computer and running the Internet update. When you install your software on the next computer, just enter the user name and password you were given when registering on the G DATA UpdateServer. Repeat this procedure on every other computer.

Please use the access data (user name and password) assigned to you when you first registered for Internet updates for all PCs. Please proceed as follows:

- 1** Start the G DATA Software.
- 2** Go to the **SecurityCenter** and click on **Update virus signatures**.
- 3** In the window that now opens, please enter the access data that was sent to you by email. If you then click on **OK**, your computer will be licensed.

## Licence renewal

A few days before your licence expires, an information window appears in the task bar. If you click this, a dialogue window opens in which you can extend your licence easily in a few steps. Just click on the **Buy now** button, complete your data and your virus protection will be guaranteed again immediately. You will then receive the invoice in the next few days via email as a PDF.

**Note:** This dialog only appears at the end of the first year. Thereafter your G DATA license will be automatically extended every year. You can cancel this extension service at any time without giving reasons.

## Changing computers

You can use your existing access data to use your G DATA product on a new or different computer. Just install the software and enter the access data. The update server will set up a connection to the new computer in this case. If your G DATA software is still on your old computer, the license must be transferred from the old computer to the new one.

**Note:** The number of licence transfers is limited – when the limit is reached the licence is completely blocked, so that no more updates of any kind can be downloaded.

## Copyright

Copyright © 2017 G DATA Software AG

Engine: The Virus Scan Engine and the Spyware Scan Engines are based on BitDefender technologies © 1997-2017 BitDefender SRL.

OutbreakShield: © 2017 Commtouch Software Ltd.

[G DATA – 24/07/2017, 10:12]