Table of contents

General

In these days of global networking and the massive security risks this incurs, the subject of virus protection is no longer just for IT specialists. Rather it has to be considered within the context of comprehensive, company-wide risk management at the highest level of management. Computer network downtime caused by a virus strikes a company where it is most vulnerable. The result: downtime for business-critical systems, loss of success-related data, loss of important communication channels. Computer viruses can cause damage to a company that it can never recover from!
G Data can provide high-end virus protection for your entire network. For years G Data products' leading security capabilities have been awarded terrific scores in numerous tests. G Data business software is consistently based on central configuration and administration plus as much automation as is possible. All clients, whether they are workstations, notebooks or file servers, are controlled centrally. All client processes run invisibly in the background. Automatic Internet updates enable extremely fast reaction times in the event of a serious virus attack. Central control via the G Data AntiVirus ManagementServer makes installation, settings, updates, remote control and automation possible for the entire network. This reduces the workload on the system administrator and saves time and money.

We wish you successful, secure work with your G Data business software.

Your G Data Team

PremiumHotline

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

USA support: **www.gdata-software.com**

United Kingdom support: **www.gdatasoftware.co.uk**

International support: **www.gdatasoftware.com**

Internet clinic

If you discover a new virus or an unknown phenomenon, always send us this file via the quarantine function in the G Data software. We will analyse the virus and send you a countermeasure as quickly as possible. We will of course treat the data you have sent us with the utmost confidence and discretion.

The return address for responses from G Data Security Labs can also be defined in the **Email settings** area.

First steps

In the event of an acute virus threat first run a **G Data boot scan** on the affected computers.

- Then install the **G Data ManagementServer** on your server. When installing the G Data AntiVirus ManagementServer the **G Data Administrator** is automatically installed on the server. The G Data AntiVirus ManagementServer can be controlled with this program. To guarantee optimal protection, the computer should always be accessible (switched on) and available for automatically loading virus signatures via an Internet connection. Installing the G Data AntiVirus ManagementServer on a server operating system does not have to occur (see **System requirements**).
- Now carry out the **online registration**. Without online registration, no software updates can be performed.
- When the G Data AntiVirus Administrator is first started on the server, the **Setup wizard** also starts. With it, the **client software** can be installed directly on the desired clients in your network. All settings undertaken by the Setup wizard can also be changed later.
- If problems arise with the **remote installation** of the clients, the client software can naturally also be installed on the clients with the aid of the G Data CD/DVD or a self-created client install package. So that the server is also protected against virus attacks, installation of the client software is also recommended for the server.
- After setup and installation of the client software has taken place on the connected machines, virus protection and Internet updates of the G Data client and server software can be controlled centrally.
The G Data Administrator provides, among other things, setting options for real-time protection by the **G Data monitor** and the option to define scan jobs that regularly inspect the network for virus attacks.
- If it becomes necessary to resolve a settings problem on a client on site, the G Data Administrator can be installed on every client within the network. With that, the need to carry out all settings locally on the server no longer applies.

System requirements

The G Data system uses the **TCP/IP protocol** for the communication of client and server computer with each other.
The following minimum requirements apply both to clients and server:

G Data AntiVirus Client

- Microsoft Windows Server 2008 (32/64 bit), 1 GB available RAM
- Microsoft Windows Server 2008 R2 (64 bit), 1 GB available RAM

- Microsoft Windows Small Business Server 2011 (64 bit), 1 GB available RAM
- Microsoft Windows Essential Business Server 2008 (64 bit), 1 GB available RAM
- Microsoft Windows Small Business Server 2008 (64 bit), 1 GB available RAM

- Microsoft Windows Server 2003 (32/64 bit), 1 GB available RAM
- Microsoft Windows Small Business Server 2003 (32/64 bit), 1 GB available RAM

- Microsoft Windows 7 (32/64 bit), 1 GB available RAM
- Microsoft Windows Vista (32/64 bit), 1 GB available RAM
- Microsoft Windows XP (SP2 or higher, 32 bit), 512 MB available RAM

- Linux, SMB 2.6.17 and beyond: Ubuntu 6.10-9.04, Debian Etch/Lenny, SuSE/SLES 10/11, RHEL 5.3/Fedora 7-10, 512 MB available RAM
- Linux, WS 2.6.25 and beyond: Ubuntu 8.10-9.10, Debian Lenny, SuSE/SLES 11, Fedora 9-12, 512 MB available RAM

For **Linux computers** that operate as file servers and provide Windows authorisations to different clients (via the **SMB protocol**), a module can be manually installed that controls access to the cleared areas and carries out a file scan with every access event, so no malware can migrate from the **Samba server** to the Windows clients (or vice versa).

G Data ManagementServer

- Microsoft Windows Server 2008 (32/64 bit), 1 GB available RAM
- Microsoft Windows Server 2008 R2 (64 bit), 1 GB available RAM
- Microsoft Windows Small Business Server 2011 (64 bit), 1 GB available RAM
- Microsoft Windows Essential Business Server 2008 (64 bit), 1 GB available RAM
- Microsoft Windows Small Business Server 2008 (64 bit), 1 GB available RAM
- Microsoft Windows Server 2003 (32/64 bit), 1 GB available RAM
- Microsoft Windows Small Business Server 2003 (32/64 bit), 1 GB available RAM
- Microsoft Windows 7 (32/64 bit), 1 GB available RAM
- Microsoft Windows Vista (32/64 bit), 1 GB available RAM
- Microsoft Windows XP (SP2 or higher, 32 bit), 1 GB available RAM

G Data MailSecurity

- Microsoft Windows Server 2008 (32/64 bit), 1 GB available RAM
- Microsoft Windows Server 2008 R2 (64 bit), 1 GB available RAM
- Microsoft Windows Small Business Server 2011 (64 bit), 1 GB available RAM
- Microsoft Windows Essential Business Server 2008 (64 bit), 1 GB available RAM
- Microsoft Windows Small Business Server 2008 (64 bit), 1 GB available RAM
- Microsoft Windows Server 2003 (32/64 bit), 1 GB available RAM
- Microsoft Windows Small Business Server 2003 (32/64 bit), 1 GB available RAM
- Microsoft Windows 7 (32/64 bit), 1 GB available RAM
- Microsoft Windows Vista (32/64 bit), 1 GB available RAM
- Microsoft Windows XP (SP2 or higher, 32 bit), 1 GB available RAM

G Data MailSecurity (plug-in for Microsoft Exchange 2010)

- Microsoft Windows Server 2008 (64 bit), 1 GB available RAM
- Microsoft Windows Server 2008 R2 (64 bit), 1 GB available RAM

- Microsoft Windows Small Business Server 2011 (64 bit), 1 GB available RAM
- Microsoft Windows Essential Business Server 2008 (64 bit), 1 GB available RAM
- Microsoft Windows Small Business Server 2008 (64 bit), 1 GB available RAM

G Data MailSecurity (plug-in for Microsoft Exchange 2007 x64)

- Microsoft Windows Server 2008 (64 bit), 1 GB available RAM
- Microsoft Windows Server 2008 R2 (64 bit), 1 GB available RAM

- Microsoft Windows Small Business Server 2011 (64 bit), 1 GB available RAM
- Microsoft Windows Essential Business Server 2008 (64 bit), 1 GB available RAM
- Microsoft Windows Small Business Server 2008 (64 bit), 1 GB available RAM

- Microsoft Windows Server 2003 (64 bit), 1 GB available RAM
- Microsoft Windows Small Business Server 2003 (64 bit), 1 GB available RAM

-

G Data boot scan

The **G Data boot scan** will help you fight viruses that have embedded themselves prior to installation of the antivirus software on your computer and that may prevent the **G Data software** from being installed. This is why there is a special version of the **G Data software** that can be run before the system starts.

What do I do if my computer will not boot from the CD/DVD? If your system will not boot from the CD/DVD-ROM, you will need to set this option up first. This is done in the **BIOS**, a system that is launched before your operating system. To make changes here, proceed as follows:

1. Switch your computer off.
2. Restart your computer. Usually you reach the BIOS setup by pressing the **DEL** button as the computer is booting up (and sometimes the **F2** or **F10** button as well). The computer manufacturer's documentation will provide more information on this.
3. You can find out from your mainboard manufacturer's documentation how to change settings in your BIOS set-up. The result should be the boot sequence **CD/DVD-ROM:, C:** , meaning that the CD/DVD-ROM drive becomes the **1st boot device** and the hard disk partition with your Windows operating system on it becomes the **2nd boot device**.
4. Save the changes and restart your computer. Your computer is now ready for a boot scan.

For the **G Data boot scan** itself, proceed as follows:

1a **G Data boot scan using the software CD**: Insert the **G Data software DVD** into the drive. In the start window that opens, click **Cancel** and turn off the computer.

1b **G Data boot scan using a G Data boot CD you have created yourself**: To do this you must first install the build software for the G Data boot CD. This must be on a system on which a G Data AntiVirus Client with up-to-date signatures has been installed; follow the G Data boot CD wizard instructions.

After this first step the boot scan in all three scenarios will proceed identically:

2 Restart the computer. The **G Data boot scan** start menu will appear.

3 Use the arrow keys to choose the **G DATA boot CD** option and confirm your choice with **Enter**. A Linux operating system is now started from the CD/DVD and a **G Data special version** for boot scans appears.

If you are having problems with the program interface display, restart your computer and choose the **G DATA boot CD – alternative** option.

4 The program now suggest updating the virus signatures.

Click **Yes** and perform the update. As soon as the data has been updated via the Internet, you see the message **Update complete**. Now exit the update screen by clicking the **Close** button.

The automatic **Internet update** is available if you are using a **router** that assigns IP addresses automatically (**DHCP**). If the Internet update is not possible, you can also run the **G Data boot scan** using old virus signatures. However, in that case, you should perform a new boot scan with updated data as soon after installing the **G Data software** as possible.
If you have created a G Data boot CD yourself, the virus signatures are of the latest update status that the G Data AntiVirus Client had loaded at the time the boot CD was created.

5 You will now see the program interface. Click on the **Check computer** option to check your computer for viruses and malware. Depending on the type of computer and size of the hard drive, the boot scan can take an hour or more.

6 If the G Data software finds any viruses, use the option provided in the program to remove them. Once the virus has been removed *successfully*, the original file is available again.

7 After completion of the virus check, click on the **Exit** button then select **Restart**.

The **Exit** button is located on the bottom right of the Linux program interface.

8 Remove the **G Data boot CD** from the drive.

9 Switch off your computer again and restart it. Your computer will now restart with your default operating system. The G Data software can now be installed on a virus-free system.

Installation

Start Windows and insert the G Data DVD in your DVD drive. An installation window will open automatically. Close all other programs before you start installing the G Data software. Errors or termination could occur if, for example, programs are left open that access data that the G Data software requires for the installation. After you have clicked on the **Install** button, a screen appears where you select which of the G Data software components you want to install. The following installation options are available:

- **G Data ManagementServer**: Firstly the **G Data AntiVirus ManagementServer** needs to be installed on the computer, which will be managing all G Data-related settings and updates. The G Data AntiVirus ManagementServer lies at the core of the G Data architecture: It administers the clients, automatically requests the latest software and virus signature updates from the G Data UpdateServer and controls the virus protection within the network. On installing the G Data AntiVirus ManagementServer, the **G Data Administrator software** is automatically installed, which is used to manage the G Data AntiVirus ManagementServer.
- **G Data Administrator**: The **G Data Administrator** is the administration software for the G Data AntiVirus ManagementServer that enables management of settings and updates for all G Data clients installed on the network. The G Data Administrator is password-protected and can be installed and launched on any Windows computer in the network.
- **G Data AntiVirus Client**: The **client software** provides virus protection for the clients and runs the G Data AntiVirus ManagementServer jobs allocated to it in the background without a separate user interface. Installing the client software is generally done centrally by the G Data Administrator for all clients.
- **Create G Data boot CD**: You can use the G Data boot CD wizard to create a bootable CD for basic scanning of your computer. This scan takes place before the installed operating system is launched. Current virus signatures are used for this. You can use the G Data boot CD to run a **Boot scan**, even without the original G Data software DVD. For more information see the section entitled **G Data boot scan**.
- **G Data WebAdministrator**: The **G Data WebAdministrator** is web-based administration software for the G Data AntiVirus ManagementServer. It can be used to create settings for the G Data AntiVirus ManagementServer via a web interface in a browser.

Directions and information that you should observe when installing the individual software components can be found in the sections for the respective software components.

G Data ManagementServer

The **G Data AntiVirus ManagementServer** lies at the core of the G Data architecture: It administers the clients, automatically requests the latest software and virus signature updates from the G Data UpdateServer and controls the virus protection within the network. The G Data AntiVirus ManagementServer uses the **TCP/IP** protocol to communicate with the clients. For **Clients** that are temporarily disconnected from the G Data AntiVirus ManagementServer, jobs are automatically accumulated and synchronised at the next contact between the G Data AntiVirus Client and G Data AntiVirus ManagementServer. The G Data AntiVirus ManagementServer has a central **Quarantine** folder. Here suspicious files can be encrypted and secured, deleted, disinfected or forwarded to the **G Data Security Labs** if necessary. The G Data AntiVirus ManagementServer is managed via the **G Data Administrator**.

If you exit the G Data Administrator, the G Data AntiVirus ManagementServer continues to be active in the background and manages the processes you have set up for the clients.

Installation of the G Data AntiVirus ManagementServer

Insert the G Data DVD and press the **Install** button. Then select the **G Data ManagementServer** component by clicking on the adjoining button.

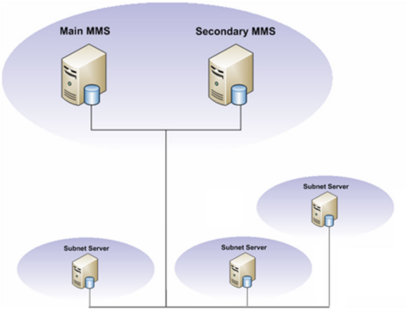
Please ensure that you have now closed all open applications in your Windows system, as otherwise they may cause problems during the installation. Now read the license agreement for the use of this software. Select **I accept the terms and conditions of the license agreement** and then click **Next** if you accept the agreement in this form. The next screen allows you to choose the installation folder.

Select server type

When selecting a server type you have the following options:

- **Install a main server**: During an initial installation, the G Data AntiVirus ManagementServer must always be installed as the **main server** (**main MMS**). The main server represents the central configuration and administration entity of the network-based virus protection architecture. The G Data AntiVirus ManagementServer provides the computers to be protected with the latest virus signatures and program updates. In addition, all client settings are carried out centrally on the G Data AntiVirus ManagementServer.
- **Install a secondary server**: When using an **SQL database** it is possible to run a **second server** (**secondary MMS**), which uses the same database as the main server. If the **main server** is unavailable for an hour or more, the clients connect automatically to the secondary server and load signature updates from it. They switch back to the main server as soon as it is available again. Both servers load the signature updates independent from one another and thus provide a safeguard against failure.
- **Install subnet server**: With large networks (e.g. company headquarters with connected branch offices) it may be sensible to operate a G Data AntiVirus ManagementServer as a **subnet server**. Subnet servers help to reduce the network traffic load between clients and the main MMS. They can be used in networks where their task is to manage the clients allocated to them. The subnet servers remain fully functional, even if the main or secondary ManagementServer is inaccessible. However, they do not load any virus signature updates autonomously.

Schematically a **server type configuration** in large networks appears as follows: Subnet servers bundle together the requests and messages of individual clients or client groups and pass these on to the main server. This is supported by a secondary server that ensures a safeguard against failure.



Database selection

Now select the database the G Data AntiVirus ManagementServer should use. Here you have the option of using an existing **SQL Server instance**, **Microsoft SQL Express** or an **integrated database** (if there is still a database from an earlier installation available).

> A server operating system is not absolutely necessary. The **SQL** variant is provided primarily in larger networks with a client number of **>1000**.
>
> The **SQL Express** variant is provided in networks with a client number of **<1000**.

Computer name

Now check the **name** of the computer on which the G Data AntiVirus ManagementServer is being installed. This computer must be addressable by the clients in the network via the name given here. If the correct name is not given here, change the entry under **Name** as appropriate.

Product activation

Product activation occurs during installation. This enables updates to be loaded after exiting the installation.

- **Enter registration number**: If you are installing the G Data software for the first time, select this option and enter the registration number for the product. Depending on the type of product, you can find this in the licence document (MediaPack) or order confirmation. In case of doubt contact your dealer or the relevant distributor.

  On entering the registration number your product is enabled. The access data generated is displayed following successful registration. **Be sure to make a note of this access data!** Following successful registration it is no longer possible to re-enter the licence key.

  If you have problems entering your registration number, please check if you have entered it correctly. Depending on the font used, a capital "I" (for India) is often misread as the number "1" or the letter "l" (for Lima). The same applies to: "B" and "8", "G" and "6", "Z" and "2".

- **Enter access data**: If the G Data software has already been installed once, you will have received access data (**user name** & **password**). To reinstall the G Data software, enter the access data here.

  You do not receive access data on repurchasing the product!

- **Activate later**: If you just want to look over the software first or if the access data is temporarily unavailable, the installation can take place without entering the data. However, if you do so, no Internet updates are loaded by the software, and you do not have proper protection against malware. You can enter your registration number or access data subsequently at any time, as soon as you run an update. Please note: if the software has been installed without being activated, only the G Data AntiVirus components are available, even if you have purchased G Data ClientSecurity or G Data EndpointProtection. The additional components are activated and available as soon as you register the software. See also the **Notes on subsequent activation of the G Data software**.

  The G Data software can only effectively protect your computer if it is completely up-to-date. Using the software without activating it will only give you insufficient protection.

Database type configuration

This installation step only occurs if you reinstall the G Data AntiVirus ManagementServer or if an **SQL database** is already installed on the computer. Usually it is sufficient to close this info box by clicking on the Close button.

Installation completion

This is ready for operation after the installation of the G Data AntiVirus ManagementServer. To carry out changes to the client settings, go to **Start > (All) Programs > G Data Administrator** and select the **G Data Administrator** option. This will start the administration tool for the G Data AntiVirus ManagementServer. The G Data AntiVirus ManagementServer will automatically be started every time the system is (re)started.

G Data Administrator

The **G Data Administrator** is the administration software for the G Data AntiVirus ManagementServer that enables management of settings and updates for all G Data clients installed on the network. The G Data Administrator is password-protected and can be installed and launched on any Windows computer in the network. Scan jobs, monitoring functions, modifications and settings can be managed in the G Data Administrator. Automatic client installations and software and virus signature updates are also defined here. The administrator tool for managing the G Data AntiVirus ManagementServer is accessed by clicking on the **G Data Administrator** option in the **Start > (All) Programs > G Data Administrator** program group in the Start menu.

Installation of the G Data Administrator

When installing the **G Data AntiVirus ManagementServer** the **G Data Administrator** will automatically be installed along with it on the same computer. Subsequent installation of the Administrator software on the G Data AntiVirus ManagementServer is not required.
The G Data Administrator can also be installed on every client computer irrespective of its installation on the server.
In this way, the G Data AntiVirus ManagementServer can also be serviced locally. To install the G Data Administrator on a client computer, please place the G Data DVD in the client computer's DVD drive and press the **Install** button. Then select the **G Data Administrator** component by clicking on the adjoining button.

Please ensure that you have now closed all open applications in your Windows system, as otherwise they may cause problems during the installation. After clicking on **Next**, the installation will continue; then follow the installation steps with the help of the installation wizard. After the installation, the entry **G Data Administrator** is available under **Start > (All) Programs > G Data Administrator**.

Logon

When starting the G Data Administrator, you will be prompted for the **server**, **authentication**, **user name** and **password**.

In the **Server** field, enter the name of the computer on which the G Data AntiVirus ManagementServer was installed.

Now select your **authentication**.

- **Windows authentication**: If you select this authentication option, you can log on to the G Data AntiVirus ManagementServer using your Windows administrator access user name and password.
- **Integrated authentication**: As system administrator, you can also use integrated authentication to give other people access to the G Data Administrator. This enables you to create a special account that only contains read rights, for example. You can create and administer these additional accounts via the function **User management** .

Initial program launch (Setup wizard)

When the G Data Administrator is first started the **Setup wizard** is automatically opened. This helps to set up the clients and takes you through all the necessary settings. After the initial installation, the wizard can still be started at any time via the **Setup wizard** command in the **Admin** menu.

Enable

All clients that are to be monitored by the G Data software must first be enabled. The clients to be enabled must first be highlighted and enabled by clicking on **Enable**. Some computers may not be included in the list (e.g. because the computers concerned have not been switched on for a long time or have not set up file or printer sharing). To enable these clients, enter the name of the computer in the **Computer** input field. After clicking on **Enable** the computer to be enabled appears in the client list. When all computers to be protected have been enabled, click on **Next** to move on to the next step.

Install

In the following dialogue box the checkbox for **Automatically install client software on the enabled computers** is checked. If distribution of the software on the client computers is to occur at a later time, this option must be disabled by removing the checkmark.

Internet update

The G Data AntiVirus ManagementServer can download new virus signatures and program files over the Internet. So that this activity can occur automatically, entering the **access data** that was created during the online registration is required. A detailed description for the scheduling of update intervals can be found in the section **Internet update**. There is also the possibility of automating the Internet update afterwards via the G Data Administrator program interface.

Email settings

The G Data AntiVirus ManagementServer can send potentially infected files to **G Data Security Labs** for investigation. So that this can be done at the push of a button, you need to enter the name of the **mail server**, the **port number** (**SMTP**) and the **sender address**. Responses from G Data Security Labs will be sent to this email address.

Email notification

In the event of a virus discovery on one or more clients, the network administrator can be informed via email. Enter the email address for the warning recipient. You can use the **limit** to prevent an excessive amount of email traffic in the event of a massive virus attack. Exit the wizard with **Finish**.

Automatic installation of the client software

If it is determined during setup that the **client software should be automatically installed**, there will be a request for access data for a user account that has administrator rights on the target system. After confirming the dialogue entries, the G Data AntiVirus ManagementServer tries to install the client software on all enabled computers. An information screen informs you about the installation progress and any problems.

> Depending on which product version is being used, you can also define here that the **G Data Firewall** is installed on the client PCs at the same time. The firewall is only available in **G Data ClientSecurity** and **G Data EndpointProtection**.
>
> If there are problems with **Remote installation** of the G Data Clients via the G Data Administrator, there is also the option of using the G Data DVD or one of the self-generated client installation packages for installing the client software on the client computers. For more information see the section entitled **Install G Data Client**.
>
> A special client software version for **Linux clients** is available. For more information, see the section **Installation of the client software on Linux computers** in the annex of this documentation.

See also **Install G Data AntiVirus Client**

Other program starts (access password)

You can invoke the G Data Administrator to control the G Data AntiVirus ManagementServer by clicking the **G Data Administrator** entry in the **G Data** program group in the start menu. When you start the G Data Administrator, you will be asked for the server and password. In the **Server** field, enter the name of the computer on which the G Data AntiVirus ManagementServer was installed.

The Administrator program interface will now open. Its functions are explained in the following sections.

G Data Administrator program setup

The G Data Administrator interface is subdivided as follows: The **Client selection area** found on the left displays all clients on which the G Data Client software is installed. To the right of this, one can switch over to the respective **Task areas** via tabs. The content of the task area normally relates to the computer highlighted in the client selection area or to the selected group of clients. Above these columns a **Menu bar** for global functions can be seen, which can be used in all fields of activity.

> When administrating **Linux clients**, which are installed on **Samba servers**, functions which, for example, are involved in handling emails are blocked because these are not required in the context of a file server. Functions which cannot be adjusted for Linux clients are highlighted using a red exclamation mark in front of the corresponding function.

Menu bar

The menu bar contains global functions that can be used in all task areas. Tasks are divided into the following areas:

- **Admin**
- **Clients**
- **Tasks** (only in the task area **Tasks**)
- **Reports** (only in the task area **Reports**)
- **Client settings** (only in the task area **Clients**)
- **Firewall** (only in the task area**Firewall**, if you are using a software version with a firewall)
- **Options**
- **? (Help)**

Admin

Basic user management and printer functions and the **Setup wizard** are available in the Admin menu.

Setup wizard

The Setup wizard enables you to select and enable clients in the network for which the G Data software should provide virus protection. The Setup wizard is explained in detail in the section **Initial program launch (Setup wizard)** .

Display log

In the **log file** you will find an overview of the latest completed G Data software actions. All relevant information is displayed here. The log display can be filtered according to the following criteria:

- **Log view**: specify here whether you would like to see a log of client or server procedures.
- **Computer/group**: Specify here whether you would like to view a log for all clients or groups or only individual areas.
- **Procedure**: Here you can define whether you would like to view all logged information or only notifications on specific topics.
- **Time**: Specify the from/to time here for which log information should be viewed.

The **Update** field is to specify that procedures which occur while viewing the log file are also listed. All procedures first appear in a chronological sequence and can be easily sorted according to specific criteria by simply clicking on the respective column title. The column according to which current sorting is carried out, is indicated by a small arrow symbol.

User management

As system administrator you can allocate additional user accesses for the G Data Administrator interface. Click on the **New** button, then enter the user name, the **authorisations** for this user (**Read/write** or **Read only**), define the **account type** (**integrated login**, **Windows user**, **Windows user group**) and enter a **password** for this user.

Manage server

Via Manage server you can assign **clients** to individual **subnet servers**, which then bundle the communication of these clients with the **main server** and in this way optimise network use. You can install subnet servers using this menu. By clicking the **Assign clients** button, you can assign existing clients to the defined subnet servers.

> The allocation of clients to subnet servers is independent of the grouping of clients. Therefore clients that are assigned to different subnet servers can nevertheless be divided into groups.

Subnet server synchronisation

To enable possible changes even outside the regular communication intervals of server and subnet server, the subnet server synchronisation can also be carried out manually.

Print templates

Here you can undertake comprehensive settings for the printout of log and statistical functions and save them in templates that can be used independently of each other.

> Depending on the selected **field of activity**, you have various selection dialogues and setting options. Printing options are not available in every task area.

Exit

This function closes the G Data Administrator. The G Data AntiVirus ManagementServer remains in operation and manages virus protection on the network in accordance with the settings.

Clients

In the clients menu, you can create settings for working with the clients and groups that are to be administered.

Update

You can use the **Update** function to track changes in the network that occur during the time you are using the G Data Administrator.

Display disabled clients

Clients that you have not **enabled** can be rendered visible again using this function. In doing so, **disabled clients** are shown as translucent icons.

In contrast, the **enabled clients** are defined by fully coloured icons.

Enable client

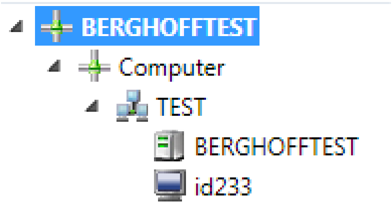
If you select a disabled *G Data Client* (represented by a translucent icon) and click on **Enable client**, it will be enabled.

As soon as a client has been enabled, a client can be installed. Enabling does not provide any virus protection. After successful installation scan jobs can be defined and client settings made for the client.

If no client has been highlighted in the client selection area, a dialogue field appears when you activate this function where you can enter the name of the client you want to enable.

Create new group

Use this command to create a **group**. Clients can be combined in groups and their settings specified in groups. After selecting this option and the issuing of a group name, clients can be assigned to the new group.



BERGHOFFTEST
Computer
TEST
BERGHOFFTEST
id233

Clients can be assigned to a group by dragging and dropping the desired client in the client list onto the corresponding group with the mouse.

Edit group

This option opens a dialogue box where the **Add** and **Remove** buttons can be used to add clients to groups or remove them from groups. Only available when a group is selected in the client selection area.

Delete

Individual clients can be removed from the client list with the **Delete** command.. The G Data Client is not uninstalled by removing the client from the list.

To delete a group, all of its included clients must be either disabled or moved to others groups as necessary. Only empty groups can be deleted.
Disabled clients can be made visible again via the **Display disabled clients** function.

Search for computer

This function can be used to search for computers within an **IP space** in the network. Enter the **Start** and **End IP address**. You then have the option of activating the computers that were found. On one hand, you have the option of activating these via your computer names or directly addressing them via the IP address. The respective client then appears with his IP address in the client selection area.

Create G Data Client installation packet

This function can be used to create an installation packet for the G Data AntiVirus Client. The packet is an individually executable file **(GDClientPck.exe)**, which can be used to install a new client on a computer to protect it without any further user interaction being needed. The installation packet, for example, is capable of allocating the client to all computers in a domain via a login script.

> The packet always contains the current client version on the server.
>
> Depending on which product version you are using, you can install the **G Data Firewall** on the client PCs via remote installation at a later date.
>
> It is absolutely essential that the installation packet is copied to the target computer and launched there with administrator rights.

Options

In the Options menu you have access to basic program settings.

Internet update

You can specify settings for Internet updates to the virus databases and the G Data software program files from here. In the tab ***Login data and settings*** , enter the access data that was created during the **online registration**. During the Internet update, the current virus definitions are loaded from the G Data UpdateServer and saved on the G Data AntiVirus ManagementServer. Distribution of the virus signatures to the clients is managed from the task area **Clients**. The Internet update ensures that current virus signatures and the latest program files are always available.

Virus database

All clients have their own local copy of the virus database, so that virus protection is also guaranteed when they are offline (i.e. no connection to the G Data AntiVirus ManagementServer or the Internet is available). **Updating** of the files on the clients takes place in two steps, which, of course, can both be automated. In the first step, the latest files from the G Data UpdateServer are copied to a folder on the G Data AntiVirus ManagementServer. In the second step, the new files are distributed to the clients (see task area **Clients**).

- **Update status**: By clicking this button, you can, if necessary, update the virus signature status display on the client, if changes in the display have not yet been adopted.
- **Start update now**: By clicking the button **Start update now** you can carry out an immediate update of the virus database. In doing so, the current virus signatures are downloaded and distributed to the clients by the G Data AntiVirus ManagementServer afterwards.
- **Automatic updates**: As with virus checks, you can also let the Internet updates run automatically. To do this check the checkbox next to **Run update periodically** and specify when and with what cycle the update is to be carried out.

> To enable automatic updating, your G Data AntiVirus ManagementServer must be connected to the Internet or you must enable the G Data software to carry out an automatic dial-up. To do this, under **Login data and settings** as necessary, enter the **user account** and **proxy settings**.

Program files

When a program update is ready for the Client software from G Data, you can allow the client update to be performed automatically by the G Data AntiVirus ManagementServer.. **Updating** the files on the clients takes place in two steps, which can both be automated. In the first step, the latest files from the G Data UpdateServer are copied to a folder on the G Data AntiVirus ManagementServer. In the second step, the new files are distributed to the clients where the client is updated (see **Clients task area**).

- **Update**: By clicking the **Update** button, you can, if necessary, update the software version status display on the client, if changes in the display have not yet been adopted.

- **Update now**: By clicking the button **Update now** you can carry out an immediate update of the client software. In doing so, the current client files are downloaded and distributed to the clients by the G Data AntiVirus ManagementServer afterwards.
- **Automatic updates**: As with virus checks, you can also let the client software Internet updates run automatically. To do this check the checkbox next to **Run update periodically** and specify when and with what cycle the update is to be carried out.

> To enable automatic updating, the G Data AntiVirus ManagementServer must be connected to the Internet or you must enable the G Data software to carry out an automatic dial-up. To do this, under **Login data and settings** as necessary, enter the **user account** and **proxy settings**.
>
> **Note**: To update the G Data AntiVirus ManagementServer program files, please select the **G Data AntiVirus ManagementServer** program group, then select the **Internet update** entry from the start menu. The G Data AntiVirus ManagementServer can only be updated via this entry. In contrast, the G Data Client software can also be updated via the G Data Administrator.

Login data and settings

With your **online registration** you will receive your access data for updating the virus databases and program files from **G Data**. Enter these under **User name** and **Password**. The **version check** (enabled by default) guarantees with every Internet update that the current virus database is copied and that the latest program files are used. In general the version check should always be switched on because it prevents the downloading of unnecessary large updates. If, however, problems arise with virus databases, switch off the version check. In this way, the current version of the virus database will be automatically transferred to your server during the next Internet update. By clicking on the User account and proxy settings **button** you open a window in which access data for the Internet and network can be entered.

> **Warning**: You should only make entries here if problems occur when using the G Data software standard settings (e.g. due to the use of a **proxy server**) and an Internet update cannot be executed.

Required for the user account is the information **user name**, **password** and **domain**. For logging on to the **proxy server**, the port (usually 80) and - if different from the user account - entry of the user name and password for the proxy server are required.

> **User account** is an account for the computer on which the ManagementServer is installed.
>
> The G Data software can use the **Internet Explorer connection data** (from version 4). First configure **Internet Explorer** and check whether the test page of our update server is accessible: **http://ieupdate.gdata.de/test.htm**. Finally switch off the option **use proxy server**. Under **User account** enter the account for which you have configured Internet Explorer (as the account with which you have logged in to your computer).

Alarm notifications

If a new virus is found, the G Data AntiVirus ManagementServer can automatically send alarm notifications via **email**. The settings required to do this are made here.

Email settings

Enter the name of your mail server, **SMTP server** and the **port** (normally 25). In addition a (valid) sender address is required so emails can be sent.

> This email address will also be used for responses from **G Data Security Labs** .

Email notification

Enable email notification by checking the **Send alarm notifications by email** checkbox and entering the email address for the notification recipient in **Recipient**. You can use the **limit** to prevent an excessive amount of email traffic in the event of a massive virus attack.

Update rollback engine A / B

Where a false alarm or similar problems occur, it can, in rare cases, make sense to block the latest **update of the virus signatures** and use a previous virus signature update instead. The G Data AntiVirus ManagementServer saves the last updates from each AntiVirus engine. Should the latest update for engine A or B result in problems, the network administrator can block the latest update for a certain time interval and instead of this distribute a prior signature update to the clients and subnet servers.

> On clients that are not connected to the G Data AntiVirus ManagementServer (e.g. notebooks used in business travel), **no** rollbacks can be carried out. A block of new updates from the server to the client cannot be retracted without contacting the G Data AntiVirus ManagementServer.
>
> The number of rollbacks to be saved can be specified in the area **Server settings**. The last five signature states are saved by default.

Server settings

Here you can carry out settings for synchronisations and automatic deletion operations.

Settings

You will find the following options in the settings area:

- **Rollbacks**: Indicate here how many of the updated virus signature updates you would like to hold as a reserve for **Rollbacks**. The default value here is the last five signature updates for each engine.
- **Automatically clean**: Here you can define that: **log entries**, **scan logs** and **Reports** are automatically deleted after a specified period of time.

Synchronisation

In the Synchronisation area you can define the synchronisation interval between clients, subnet servers and servers:

- **Clients**: Here you enter the time interval in which the clients are synchronised with the server. If you set the checkmark next to **Notify client if settings have been changed on the server**, the user receives a message on the client computer that changes have been carried out. The default value is five minutes.
- **Subnet server**: in this area you can define the intervals for communication between server and subnet server. If you check the checkmark next to **Send new reports to the main server immediately**, the reports will be transferred to the main server immediately, independently of the settings made here.

Load limit

If the checkmark next to the entry **Enable load limit** is set, you can specify how many clients can simultaneously perform the actions listed under it. The load can thereby be distributed so that, for example, simultaneously loading updates does not result in a latency increase in the network.

Backup

Thresholds for warnings that are issued when the values entered are reached are set up in the **Quota** area. Here you can set up how much storage space must be free on the server before a warning or error message is issued. This makes sense if, for example, a certain amount of storage space must always be available on the hard disk for applications. If, for example, the value 1500 is entered as the **Threshold for client warnings**, a warning is displayed in the G Data Administrator under **Reports** that only 1500 MB of storage space remains available. If a **Threshold for client error reports** is entered, on reaching that value older backups are deleted to create storage space for new backups. In this case the oldest backup is deleted first (FIFO principle).

Furthermore, under **Server backup paths** a path can be entered on which all backups being generated are stored. If no path is entered here, all backups are stored under **C:\ProgramData\G DATA\AntiVirus ManagementServer\Backup** or **C:\Documents and Settings\All Users\Application Data\G DATA\AntiVirus ManagementServer\Backup**
.

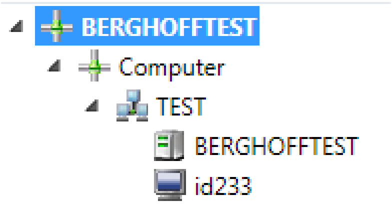
As all backups generated by the G Data software are encrypted, there is also the option of exporting passwords for the backups and saving them for later use. The **Import backup archives** button enables access to backups that are stored in other folders.

Help

Here you can access information on the program and also have the option of accessing the **G Data software** online help function.

Client selection area

All clients, servers and defined groups in your network are listed here. As in Windows Explorer, groups that have subdivisions appear with a small plus symbol. If you click on this, the directory structure opens up and enables the view of the structure below it.



- BERGHOFFTEST
  - Computer
    - TEST
      - BERGHOFFTEST
      - id233

Clicking the minus symbol closes the subdivision again. The following icons are visible in the Directory selection:

Network icon

Group

Server (activated)

Server (disabled)

Client (activated)

Client (disabled)

Linux client (enabled)

Linux client (disabled)

Non-selectable devices: For example, network printers fall under this category

In the toolbar you will see the most important commands from the **Menu bar** displayed as clickable icons.

Update view: Use **Update** or the **F5** key to update the display of the Administrator interface at any time, for example to take account of current changes to the display.

Display disabled clients: Select this button to display disabled computers as well. You can recognise the disabled computers by their greyed-out icons. Computers without file sharing or printer sharing are not normally shown.

New group: The enabled computers can be linked into **groups**. Easily distinguishable security zones can be defined since all settings can be made for both single clients and for entire groups. To create a new group, first highlight the superordinate group then click on the icon displayed.

Delete: You can remove a computer from the list by highlighting it and then clicking on the **Delete** button. Note that deleting a computer does not mean that the client software is uninstalled.

Enable client: To enable a computer, highlight it in the list and select the button displayed. You can also activate computers that do not appear in the list. To do this, in the client menu select the **Enable client (dialog)** command and enter the computer's name.

AD integration

Since version 11 Active Directory integration has been available in G Data software. This imports all computer objects for the domain's organisation units. A separate group must be set up in the G Data Administrator to do this. When you right-click on the newly set-up group, the **Assign AD item to group...** menu item appears.

In the dialogue window that opens, select the **Assign to AD group** item and enter the **LDAP server** there. The **Select...** button provides a list of available servers. **Connect to other domain** is another option.

If the distribution of the clients on individual computers is meant to occur automatically immediately on connection, the **Automatically install G Data Client on activated clients** option must be activated. This option also has the effect that the client is immediately installed on every computer that is added to the Active Directory domain, as long as it meets the **minimum requirements**. The G Data AntiVirus ManagementServer compares its data status with the Active Directory every 60 minutes. This value cannot be changed.

Task areas

You have the option of administering the protection of your clients in the different task areas that you can select via the respective tabs. The settings created there always relate to the clients or groups highlighted in the **Client selection area**. The different subject fields are explained in detail in the sections below.

- **Dashboard**
- **Tasks**
- **Settings**
- **Exchange settings** (available on installing **G Data MailSecurity**)
- **Reports**
- **Clients**
- **PolicyManager** (available in the **G Data EndpointProtection** version)
- **Firewall** (available in the **G Data ClientSecurity / G Data EndpointProtection** version)
- **Statistics**

Dashboard

In the G Data software Dashboard area you can see information about the current status of the clients in the network. This information, consisting of text, figures or dates, is displayed to the right of each item.

G Data Client Status

Here you can create all the basic security settings for the clients or groups that you have highlighted in the client selection area.

✓ As long as your network is optimally configured for protection against computer viruses, you will see a green icon to the left of the entries listed here.

❗ If at least one component is not optimally set (e.g. monitor switched off or obsolete virus signatures), a warning symbol will alert you.

ℹ When the G Data program interface opens, most of the icons will occasionally be displayed in info mode for a short time. This does not mean that the network is not protected at that time.
This is actually an internal check of the virus protection status. At this time the G Data AntiVirus ManagementServer's database is being queried by the G Data Administrator.

By clicking on the respective entry, you can undertake actions right here or change to the respective task 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 icon.

Client connections

This gives you a temporal overview of the connections the relevant clients or groups have made to the G Data AntiVirus ManagementServer. You should check here that all clients are connecting to the G Data AntiVirus ManagementServer regularly.

Top 10 infected clients

The clients that appear in this list due to e.g. usage behaviour or technical circumstances should be monitored especially carefully. The appearance of one or more clients in this area can potentially indicate that the client users should be notified of possible problems or take technical measures. If infections are taking place as a result of usage behaviour, use of e.g. the **PolicyManager** (available in the **G Data EndpointProtection** program version) might be advisable.

Report status

Here you can see a visual representation of the number of infections, queries and errors in your network during the last 30 days.

Tasks

In this task area you can define tasks for virus checks on the G Data Clients . There are two different job types: **single scan jobs** and **periodic scan jobs**. Single jobs are performed once at a specific time; for the periodic jobs a **Schedule** is defined according to which they are run.

> All tasks generated on the G Data AntiVirus ManagementServer are referred to as **scan jobs** or **jobs**. These can be scanning tasks, backup tasks or restore tasks.

In the **Tasks** area all jobs appear under the name given to them by you and can be sorted according to the following criteria by simply clicking on the respective column designation. The column according to which current sorting is carried out, is indicated by a small arrow symbol:

- **Name**: The name specified by you for the job. You can enter a name of any length here and thereby precisely describe your job in order to maintain an overview when there are a large number of different jobs.
- **Computer**: You will find the name of the corresponding clients here. You can only define jobs for activated clients.
- **Group**: You can combine individual clients into groups which then use the same jobs. If you assign a job to a group, the group name appears in the overview list rather than the individual computers.
- **Status**: Here you obtain the status or the results of a job displayed in plain text. Thus, for example, you can see whether the job has just run or has been completed, and also find out whether or not viruses were found.
- **Last run**: In this column you receive information as to when the respective job was last run.
- **Time interval**: According to the **Scheduling** that you can define for every job, this states in which cycle the job will be repeated.
- **Analysis scope**: Here you find out to which **data media** (e.g. local hard disks) the analysis extends.

> In the menu bar, an additional menu entry with the following functions is available for the task area **jobs**:

- **View**: Select whether you would like to display all **jobs** or only scan jobs, only backup jobs*, only restore jobs*, only single scan jobs, only periodic scan jobs, only open scan jobs or only completed scan jobs here. For scan jobs that were defined for a **group** of clients, you can decide whether detailed information about all clients or only cross-group summaries should be displayed. Check the box next to **Display group jobs in detail** to do this.
- **Run now**: This enables you to run selected jobs independently of any scheduled jobs.
- **Cancel**: You can cancel a running job with this function.
- **Delete**: Selected jobs can be deleted using this function.
- **New**: Select whether you want to create a **one-time scan job** (single test) or a **regular scan job** (periodic test) here. You can also generate a backup or restore job.*

You can define as many different scan jobs as you would like. For performance reasons, it generally makes sense that scan jobs do not overlap.

* This depends on your product version.

Update

This function updates the view and loads the current job list from the G Data AntiVirus ManagementServer.

Single/periodic scan job

This function enables scan jobs to be defined for individual computers or computer groups. In the configuration dialogue the time, scope and additional scan settings can be defined on the relevant tabs.

Double-click on the entry to change the parameters for an available job, or select the **Properties** command from the context menu (by right-clicking the mouse). You can now change the scan job settings to what you want.

Job

Here you can specify what name the scan job should have. You can enter meaningful names here such as *Archive scan* or *Monthly scan* to unambiguously label the desired job so that it can be found again in the tabular overview. Furthermore, permissions can be granted to the users for pausing or aborting the job via the context menu of the tray. You can use the **Report scan progress to the ManagementServer** option to have the status of a scan process running on a client displayed as a percentage in the G Data Administrator. The report interval for the scan progress cannot be modified. The **Shut down client when scan job is completed; no user must be logged on** function provides another way to help reduce your administrative load. If a computer is not switched on at the specified time of a scan job, the scan job can be started by means of the option **Run scan job later if a client is not powered up at the scheduled time** if the computer is switched on after this point in time.

Time / scheduling

This tab specifies when and at what intervals the virus check should occur. If you select **On system startup** the scheduling defaults no longer apply and the G Data software will run the update each time your computer is restarted.

> Under **Daily** you can specify using the settings under **Weekdays** that the computer should only carry out a virus check on weekdays or even only every other day or on specific weekends when it is not being used for work.
>
> If a **single scan job** is created, only the option **Start at** is available. If a start time is not specified, the scan job will be started immediately after creation.

Scanner

In the Scanner menu you can find the settings with which the scan job can be executed. The following options are available:

- **Use engines**: The G Data software works with two independently operating virus analysis units. In principle, you must use both engines to guarantee optimum virus combat results. However, using a single engine does have performance benefits – analysis can be performed more quickly if only one engine is used. We recommend the setting **Both engines - performance optimised**. In this scenario, both virus scanners cooperate such that optimised detection accuracy is achieved within a minimised scanning duration.

- **In case of an infection**: Here you can specify the action to be taken if an infected file is detected. There are various options here that may or may not be suitable, depending on what the respective client computer is used for. By setting **Move file to quarantine**, an infected file is moved to a special directory that is created by the G Data AntiVirus ManagementServer. Infected files are encrypted there so that possible malware can no longer be executed. Files in **quarantine** can be disinfected by the network administrator, deleted, moved back to their original storage location or, if required, sent to the **Internet clinic** .

- **Infected archive**: Specify here how infected **archives** are to be treated. When specifying these settings, you should bear in mind that a virus in an archive will only be harmful when it is unpacked from the archive.

- **File types**: Here you can define the file types G Data should check for viruses. Please bear in mind that checking all files on a computer can take considerable time.

- **Priority scanner**: You can use the levels **high**, **medium** and **low** to specify whether virus checking by G Data should have high priority on your computer (in which case the analysis is relatively quick and other applications may run more slowly during the analysis) or low priority (the analysis requires more time, so that other applications can continue to run relatively unaffected). Depending on the time you take to run the virus analysis, different settings are useful here.

- **Settings**: Specify the additional virus analyses you want the G Data software to perform. The options selected here are generally recommended. Depending on the type of application, the time gained by omitting these checks may outweigh the slightly reduced level of security. The following configuration options are available:

Heuristics: Heuristic analysis detects viruses not only on the basis of constantly updated virus databases, but also based on detecting characteristics that are typical of most viruses. The heuristics can generate a false alarm in rare instances.

Archive: Checking of compressed data contained in archives is very time consuming and can generally be suppressed if the **G Data monitor** is 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. Nevertheless, during regular checks of the computer outside the actual usage times, checking of the archives should also take place.

Email archive: Checking of email archives is very time consuming and can generally be suppressed if the **G Data monitor** or the Outlook plug-in is enabled on the system. While accessing the archive, the monitor detects a virus that is hidden to date and automatically prevents its dissemination. Nevertheless, during regular checks of the computer outside the actual usage times, checking of the archives should also take place.

System areas: The system areas of your computer **(boot sectors, master boot record etc.)** that provide the fundamental basis for the operating system should not be excluded from the virus check as some malware can nest itself specifically in this area of the system.

Check for diallers / spyware / adware / riskware: You can use the G Data software to check your system for **diallers** and other malware programs (**spyware**, **adware**, **riskware**). This concerns, for example, programs that establish unrequested expensive Internet connections and are potentially every bit as damaging as a virus in terms of economical destruction. Spyware, for example, can record your surfing habits or even all keyboard entries (and with that your passwords) unbeknownst to you and at the next opportunity forward them to unknown people over the Internet.

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

Use all available processors: With this option, you can distribute the virus checking load on systems with multiple **processor kernels** over all the processors with the result that the virus checking runs considerably quicker. The downside to this option is that less processing power is available for other applications. This option should then only be used if the scan job is executed at times when the system is not regularly used (e.g. at night).

Analysis scope

You can also limit the virus control on the client to specific directories via the **Analysis scope** tab. In this way, for example, folders with rarely used archives can be left out and checked in a separate scan job. When so doing, the Directory selection refers to the currently selected computer and not to the selected client.

Special feature for scan jobs on a Linux file server: The root drive (/) and all authorisations will be returned with the directory selection. Scan jobs can thus be performed in a targeted manner based on selected authorisations or on file server directories selected as desired.

Delete scan jobs

The function **Delete...** deletes all highlighted jobs.

Run scan jobs again (immediately)

Select this function to re-run **single scan jobs** which have already been run or cancelled. For periodically executing scan jobs, this function causes the job to be run independently of the schedule.

Logs

Use this function to call up the logs relating to a particular client's jobs.

Show options

With a large number of different scan jobs, it is useful to show and list these according to particular criteria. The following options are available:

Show all jobs

Only show single scan jobs

Only show periodic scan jobs

Only show open scan jobs

Only show completed scan jobs

Display group jobs in detail: Displays all associated entries with group jobs. The option is only available if a group is selected in the computer list.

New scan job (Exchange)

This chapter describes how to set up scan jobs for the Microsoft Information Store. This option is only available in program versions where the G Data MailSecurity plug-in for Microsoft Exchange 2007 / 2010 has been installed. There are also two different types of scan jobs: **periodic** or **single scan jobs**. A **single scan job** is only run once, whereas a **periodic scan job** is run at regular intervals. Right-click in a free area of the window to open a context menu and click on **New**. Then select the scan type you want. After you have made your selection, the configuration dialogue for the scan job opens.

This function can be used to define scan jobs for individual Exchange servers or for groups of Exchange servers. In the configuration dialogue, the **settings**, **scheduling** and **scope** relevant to the job can be defined on the relevant tabs.

Double-click on the entry to change the parameters for an available job, or select the **Properties** command from the context menu (by right-clicking the mouse). You can now change the scan job settings to what you want.

Settings

Here you can specify what name the scan job should have under **Job name**. You can enter meaningful names here such as *Archive mailboxes* or *Monthly check of all mailboxes* to unambiguously label the desired job so that it can be found again in the tabular overview. You can use the **Report scan progress to the ManagementServer** option to have the status of a scan process displayed as a percentage in the G Data Administrator. The report interval for the scan progress cannot be modified.

Scanner

In the Scanner area you can find the settings with which the scan job can be executed. The following options are available:

- **Use engines**: The G Data software works with two independently operating virus analysis units. In principle, you must use both engines to guarantee optimum virus combat results. However, using a single engine does have performance benefits – analysis can be performed more quickly if only one engine is used. We recommend the setting **Both engines - performance optimised**. In this scenario, both virus scanners cooperate such that optimised detection accuracy is achieved within a minimised scanning duration.

- **In case of an infection**: Here you can specify the action to be taken if an infected file is detected. There are various options here that may or may not be suitable, depending on what the respective client computer is used for. By setting **Move file to quarantine**, an infected file is moved to a special directory that is created by the G Data AntiVirus ManagementServer. Infected files are encrypted there so that possible malware can no longer be executed. Files in **quarantine** can be disinfected by the network administrator, deleted, moved back to their original storage location or, if required, sent to the **Internet clinic** .

- **Infected archive**: Specify here how infected **archives** are to be treated. When specifying these settings, you should bear in mind that a virus in an archive will only be harmful when it is unpacked from the archive.

- **File types**: Here you can define the file types G Data should check for viruses. Please bear in mind that checking all files on a computer can take considerable time.

  Heuristics: Heuristic analysis detects viruses not only on the basis of constantly updated virus databases, but also based on detecting characteristics that are typical of most viruses. The heuristics can generate a false alarm in rare instances.

  Archive: Checking compressed data in archives is a very time-consuming process and can generally be omitted if the G Data AntiVirus Client is installed and enabled on your system. The monitor can detect a previously hidden virus while the archive is being unzipped and can automatically prevent it from spreading. Nevertheless, during regular checks of the computer outside the actual usage times, checking of the archives should also take place.

Time / scheduling

This tab specifies when and at what intervals the virus check should occur. If you select **On system startup** the scheduling defaults no longer apply and the G Data software will run the update each time your computer is restarted.

> Under **Daily** you can specify using the settings under **Weekdays** that the computer should only carry out a virus check on weekdays or even only every other day or on specific weekends when it is not being used for work.

If a **single scan job** is created, only the option **Start at** is available. If a start time is not specified, the scan job will be started immediately after creation.

Analysis scope

You can also limit the virus control on the client to specific mailboxes via the **Analysis scope** tab. For example, this allows archived mailboxes to be left out and checked in a separate scan job. If you set up public folders in your Exchange environment, you can include these in the virus check by checking the box next to **Scan public folders**.

Backup job

In this area you can create settings for backup jobs. You can set up **full backups** or **partial backups** (differential) at defined times.

To be sure of having constant backups of data on the network, it is recommended that you run a daily backup, so that the last backed-up data version is always available in the event of loss of data (e.g. by inadvertently deleting a file). Wherever possible, a backup should be physically and logically separated from the production environment so that the data continues to be secure even in the event of a total systems failure.

The G Data Backup provides a file backup solution. It is not possible to back up an image of an entire client system.

Double-click on the entry to change the parameters for an available job, or select the **Properties** command from the context menu (by right-clicking the mouse). You can now change the backup job settings to what you want.

Select directories

A **name** for the backup job must first be entered. It is recommended that you use a self-explanatory name to make it easier to identify individual backup jobs. All directories that need to be included in the data backup are listed under the **Select directory** option - individual clients can be selected using the **Client** dropdown menu. If **Local search** is selected, the network administrator can search the folder structure on the computer on which the G Data Administrator is running. Individual directories are added to or removed from the backup using the **Add** and **Remove** buttons. Directories that are added are displayed on the right-hand side under **Selected paths**. Enabling the **User directories** option automatically includes all directories under **C:\Users** or **C:\Documents and Settings**.

There is also the option of importing lists of directories to be backed up. The paths to the directories to be backed up must be entered as absolute paths in a *.txt file. Each path must be in a separate line. The **Import** button can be used to import the list directly into the **Selected paths** without needing to make any other selections. Similarly, the **Export** button can be used to save the scope of a data backup to a *.txt file for later use. Alternatively, the path to the directory to be backed up can also be entered directly in the **Current path** input field.

Scheduling

Scheduling of individual backup jobs allows for the creation of backups in specified chronological intervals. These range from a full backup, which is carried out once, to a partial backup, which can be created daily. In addition, there is an option that allows a backup job to be postponed if the system is running in battery mode. It is recommended that you enable this option on mobile computers to prevent burdening the battery with a backup job. The backup will be made up as soon as the client is connected to the power supply again. If a client is not connected to the ManagementServer at the time of the backup, the backup will initially be buffered on the client. The partition containing the most free storage space will be used for this. The backup will be transferred during the next contact with the ManagementServer. If a client computer is not switched on at the time of the backup, the backup will be made up as soon as the computer is switched on.

Provided nothing else is indicated in the **Server settings**, backups on the ManagementServer will be saved in the directory **C:\ProgramData\G DATA\AntiVirus ManagementServer\Backup** or **C:\Documents and Settings\All Users\Application Data\G DATA\AntiVirus ManagementServer\Backup**.

> If not enough storage space is available on the client at the time of the backup, a corresponding error message will be displayed in the G Data Administrator.

Options

Certain file types can be excluded from the backup under **Exclude files**. Thus **directories** that contain **temporary files** can be excluded. Also the exclusion of files assigned the **File attribute Temporary file** or **System file**. Certain file types can also be specifically excluded. For this, the extension of the file type that is to be excluded from the backup (e.g. *.mp3) must be indicated under **File type**. The entered file types can be added to the list of file types to be excluded via the **Add** button. Accordingly, files that should be backed up after all (contrary to earlier settings) can be removed from the list again via the **Delete...** button. If the generated backup should be saved in a particular directory prior to transmission to the ManagementServer, this specification can be indicated under **Cache**. If the option **Use client standard path** is enabled and an absolute path is indicated, the backup will be buffered in the specified directory. If this option is not enabled, the G Data Client will always save the backup on the partition containing the most free disk space. The directory **G Data\Backup** will then be created in the root directory of the partition.

Settings

In this task area options for e.g. Internet updates or local authorisations for changing settings for all clients, individual clients or a group of clients can be set. You can use the selection box above to determine what sort of options you want to edit for this. In the **Client selection area** select the desired client for this or the group of clients that you would like to configure, then execute the desired entries and close the procedure by clicking the **Accept** button.

General

Here you have the following setting options:

G Data Client

The following functions are available:

- **Remark**: Enter a distinctive name for the relevant client
- **Display tray icon**: For terminal servers and Windows with fast user switchover you can select the sessions in which a client icon should be displayed in the taskbar: **never**, **only in the first session** or **always**. The client icon can optionally be prevented from being displayed for "normal" clients. The icon must be displayed to enable the user to have access to extended client functions.
- **User account**: The client software normally runs in a system environment. You can enter another account here to enable network directories to be scanned. To do this, the account must have administrator rights for the client.

Updates

The following functions are available:

- **Automatically update virus signatures**: Enables automatic updating of the virus database. The clients periodically check whether current virus signatures exist on the ManagementServer. If current virus signatures are available, they are automatically installed on the client.
- **Automatically update program files**: Updates the program files on the client. The client program files that the ManagementServer keeps ready are used for this. A client reboot may be necessary after updating the program files. Dependent on the setting under **Reboot after update** the client user has the option of postponing the completion of the update to a later point in time.
- **Restart after updating**: Here you specify whether the client is automatically restarted after the program files are updated (**Force reboot**), whether the user is offered the option to carry out a restart immediately or later (**display window on the client**) or whether the update of the program files is only carried out when the client is rebooted by the user (**Create report**).

Client functions

Below the permissions that the user has locally for individual client functions are allocated. Hence the user can be granted extensive or only very restricted rights for changing settings.

- **The user can run virus checks**: In an acute case of suspicion, the user can run a **virus check** on his computer as he would with a locally installed antivirus solution, independent of the ManagementServer. Results of this virus check will be transferred to the ManagementServer during the next contact with it.
- **The user can download signature updates**: If you enable this function, the user of the client computer is allowed to download virus signatures over the Internet from the context menu, without connecting to the ManagementServer.
- **The user can change email and monitoring options**: If this function is enabled, the client user has the option, in addition to the **monitor options** , of influencing the settings in a targeted way where **email security** for his client is concerned.
- **Display local quarantine**: If you allow the local **quarantine** to be displayed, the user can, if necessary, disinfect, delete or restore data that was moved into quarantine by the monitor due to virus infection or suspicion. In doing so, note that a virus is not removed by restoring a file from quarantine. This option should therefore only be made accessible on clients for experienced users.
- **Password protection for changes to options**: To prevent improper manipulation of local settings, there is the option of only permitting options to be changed when a password is entered. This allows you, for example, to prevent a user who does not usually work on the client concerned from changing the settings. The password can be allocated specifically for the relevant client or the relevant group; this password must only be shared with authorised users.

- **Update settings**: Here you can define where clients obtain their virus signature updates from. There is the option of allowing all clients to download virus signatures from the ManagementServer indiscriminately; alternatively you can grant them the right to run the updates themselves. Mixed mode is recommended for mobile workstations; i.e. when the client has a connection to the ManagementServer, it gets the updates from there. If there is no longer a connection to the ManagementServer, the virus signatures are automatically downloaded from the Internet. Furthermore, the **Settings and scheduling** button can be used to create settings for the relevant client enabling virus signatures to be downloaded as required, depending on the usage environment. The intervals at which updates are run can also be defined here.

Exception directory for scan jobs

You can define client directory exceptions here that are not to be checked during the execution of scan jobs. Archive and backup areas of a hard disk or partition, for example, can be defined as exception directories where applicable.

Exception directories can be defined for complete **groups**. If the clients in a group have defined different exception directories, new directories can be added or existing ones can be deleted. The directories specially defined for individual clients are thereby preserved. The same procedure is also used with the monitor exceptions.

Special note for Linux file servers

The root drive (/) and all authorisations will be returned with the exception directories selection. In doing so, drive, directory and file exceptions can be created.

Monitor

The monitor settings for the client selected in the **Client selection area** or the selected group can be created here. The changed settings are only saved once the **Apply** button has been pressed. Press the **Discard** button to load the current settings from the ManagementServer without accepting the changes.

> If clients within a group have different settings using parameters that have been set up differently, individual parameters can be allocated an undefined status. In this event the clients in the group have different settings for the parameter. Undefined parameters are not saved during the transfer.

The monitor really should not be disabled, as it provides real-time protection against malware. If the monitor is disabled, you no longer have this protection. It is therefore recommended that the monitor is only switched off if there is a justified reason for doing so, e.g. error detection or diagnosis.

> It is possible to define exceptions for the monitor. If an application is struggling with performance losses due to use of the monitor, exceptions can be added for the relevant program files, processes or files; excluded files are then no longer checked by the monitor. Note that, in certain circumstances, setting up monitoring exceptions can represent a security risk.

Settings

The following functions are available in the settings area:

- **Monitor status**: From here you can switch the monitor on and off. In general you should leave the monitor switched on. It forms the foundation for permanent and uninterrupted virus protection.

- **Use engines**: The G Data software works with two independently operating virus analysis units. In principle, using both engines guarantees optimum results for preventing viruses. On the other hand, using just one engine has certain performance advantages.

- **In case of an infection**: Here you can specify the action to be taken if an infected file is detected. There are various options here that may or may not be suitable, depending on what the respective client is used for.

Block file access: Neither read nor write access can be granted for an infected file.

Disinfect (if not possible: block access): An attempt is made to remove the virus; if this is not possible, file access is blocked.

Disinfect (if not possible: place in quarantine): This tries to remove the virus. If this is not possible, the file is moved to **Quarantine** .

Disinfect (if not possible: delete file): This tries to remove the virus. If this is not possible, the file is deleted. However, in the rare case of a false-positive virus message, this may lead to data loss.

Move file to quarantine: The infected file is moved to quarantine. The system administrator can then try to manually disinfect the file.

Delete infected file: This function serves as a strict measure for effectively containing a virus. However, in the rare case of a false-positive virus message, this may lead to data loss.

- **Infected archive**: Specify here how infected **archives** are to be treated. When specifying these settings, you should bear in mind that a virus in an archive will only be harmful when it is unpacked from the archive.

- **File types**: Here you can define the file types G Data should check for viruses. Please bear in mind that checking all files on a computer can take considerable time.

- **Check when writing**: Normally a virus-free system will not generate virus-infected files when writing files. However, to prevent any such eventuality, you can set up a scan procedure here for use when writing files. The huge advantage of this is that even viruses that are copied from another possibly unprotected client to an enabled directory on the client that is protected by the monitor are detected, and files downloaded from the Internet are first recognised as virus-infected when loaded and not when first run.

- **Check network access**: Here you can specify operation of the monitor in conjunction with network access. If your entire network is normally monitored by the G Data software, network access verification may be discontinued.

- **Heuristics**: In a heuristic analysis, viruses are not only detected on the basis of the constantly updated virus databases, but are also examined for characteristics typical of viruses. On the one hand, this method is an additional security benefit; on the other, it can also give rise to a **false alarm** in rare cases.

- **Check archive**: Checking compressed data in archives is a very time-consuming process and can generally be omitted if the G Data virus monitor is always enabled on your system. The monitor can detect a previously hidden virus while the archive is being unzipped and can automatically prevent it from spreading. To avoid decreasing performance with unnecessary checks of large archive files that are rarely used, you can set a size limit (number of kilobytes) for archives to be checked.

- **Check email archive**: This option should generally be disabled, as scanning email archives generally takes a long time, and if an infected email is found the mailbox is moved to quarantine or deleted - depending on the virus scan settings. Email in the mail archive should no longer be available in such a case. As the monitor blocks execution of email attachments, disabling this option does not create a security hole. When using **Outlook**, incoming and outgoing mails are also scanned using an integrated plug-in.

- **Check system areas during system start**: System areas (for example **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 DVD etc.). Generally you should have at least one of these two functions activated.

- **Check system areas on media exchange**: In general, system areas (for example **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 DVD etc.). Generally you should have at least one of these two functions activated.

- **Check for diallers / spyware / adware / riskware**: You can use the G Data software to check your system for **diallers** and other malware programs (**spyware**, **adware**, **riskware**). This concerns, for example, programs that establish unrequested expensive Internet connections and are potentially every bit as damaging as a virus in terms of economical destruction. For example, spyware can silently record your surfing behaviour or even all keystrokes (and therefore your passwords) and forward this to third parties via the Internet at the next opportunity.

- **Notify user when virus found**: If this option is enabled, when a virus is found by the monitor on the client concerned, a notification window opens informing the user that a virus has been found on his system. The file that has been found, its path and the name of the malware found are displayed there.

Exceptions

Here you can also limit client virus checking for specific directories. In this way for example, you can omit folders with archives that are seldom used, to integrate them into a special scan job. Furthermore, certain files and file types can be excluded from the virus check. The following exceptions are possible:

- **Drive**: By clicking the directory button here, you select a drive (**partition**, **hard disk**) that you do not want checked by the monitor.
- **Directory**: By clicking the directory button here, you select a **folder** (as necessary, including any **subfolder** contained within it) that you do not want checked by the monitor.
- **File**: Here you can enter the name of the file that you would like excluded by the monitor check. You can also use wildcards here.
- **Process**: If a specific process should not be monitored by the monitor, enter the name of the process concerned here.

You can repeat this procedure as many times as you wish, and you can delete or modify the existing exceptions in the **Monitor exceptions** window.

Wildcards works 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 **exe**, enter ***.exe**. For example, to protect files with different spreadsheet formats (e.g. **.xlr**, **.xls**), simply enter ***.xl?**. Or to protect files of various types that have identical initial file names, enter e.g. **text*.***. This would involve files called *text1.txt, text2.txt, text3.txt* etc.

Warning messages

Specify here whether the user on the client computer is notified when a virus is found. If the checkmark is set here, the user sees an info window that informs him of the viruses found.

Status

Here you are shown whether the changes you have made to the monitor have already been transferred to the client or the group or whether you still have to click the **Accept** button.

Behaviour monitoring

Behavior monitoring provides further protection against malicious files; unlike the monitor, it is not signature-based but analyses the actual behavior of a file. To undertake a classification, behavior monitoring uses various criteria, among others write access to the registry and the possible creation of auto-start entries. If sufficient criteria allow the conclusion to be reached that a program is at least exhibiting suspicious behavior, the action set under **If a threat is detected** will be carried out. The options **Log only**, **Halt program** and **Stop program and move to quarantine** are available here. With the setting **Log only** the program no longer continues to be impacted and a corresponding message is displayed under **Reports**.

Email

Special virus protection for email can be set up on every G Data AntiVirus Client. In doing so the default ports for the **POP3**, **IMAP** and **SMTP** protocols are monitored. Furthermore, a special **plug-in** is used for **Microsoft Outlook**. The plug-in automatically checks all incoming email for viruses and prevents infected email from being sent. By clicking on the **Apply** button, you accept the changes that have been made; **Discard** resets all the changes made. You can create individual configurations for handling mail for every client or for user groups via the G Data Administrator. In this respect, you can select from the following options:

Incoming mail

The following functions are available:

- **In case of an infection**: Here you can specify the action to be taken if an infected file is detected. There are various options here that may or may not be suitable, depending on what the respective client is used for.

- **Check received email for viruses**: By enabling this option, all emails that the client receives online will be checked for viruses.

- **Check unread mails on program start-up (Microsoft Outlook only)**: This option is used to scan emails for viruses that the client receives while it is offline. All unread email in your Inbox folder and subfolders are therefore checked as soon as you open **Outlook**.

- **Append report to received, infected mails**: As soon as one of the emails sent to the client contains a virus, you will receive the following message in the body of this mail beneath the actual mail text **WARNING! This mail contains the following virus** followed by the name of the virus. In addition, you will find the **[VIRUS]** notification before the actual subject. If you enabled the option **Delete attachment/text**, you will also be notified that the infected part of the email was deleted.

Outgoing mails

The following functions are available:

- **Check email before sending**: So that you do not send viruses from your own network via email, the G Data software also offers the option of checking outgoing emails for viruses before sending them. If a virus actually does get sent, the message **The mail [subject header] contains the following virus: [virus name]** appears. The relevant email is not sent.

- **Append report to outgoing email**: A certification report is displayed in the body of each outgoing email below the actual mail text. This reads **Virus checked by G Data AntiVirus**, provided that you have enabled the **Check emails before sending** option. Here you can also indicate the version date of the G Data AntiVirus (**version information**).

Scan options

The following functions are available:

- **Use engines**: The G Data software works with two independently operating virus analysis units, the so-called engines. In principle, you must use both engines to guarantee optimum virus prevention results. However, using a single engine does have performance benefits – analysis can be performed more quickly if only one engine is used.

- **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 emails, enabling it to close the window between a mass mail outbreak and its containment with specially adapted virus signatures, practically in real time. Under **change** you can specify whether OutbreakShield uses additional signatures to increase detection performance. In addition you can enter access data here for the Internet connection or a proxy server, which then permits OutbreakShield to carry out an automatic signature download from the Internet.

Warning messages

Notify user when virus found: You can inform the recipient of an infected message automatically. A virus alert is then displayed on his desktop.

Outlook protection

The following functions are available:

- **Protect Microsoft Outlook through an integrated plug-in**: Activation of this function inserts a new function in the client's **Outlook** program under the **Tools** menu, called **Check folder for viruses**. Regardless of the G Data Administrator settings, an individual client user can scan the currently selected email folder for viruses. In the email display window you can use **Check email for viruses** in the **Tools** menu to run a virus check of the file attachments. When the process has been completed, an information screen appears in which the result of the virus check is summarised. Here you can see whether the virus analysis was completed successfully, get information about the number of emails and attachments scanned and about any read errors, as well as any viruses found and how they were dealt with. You can hide both windows by clicking on the **Close** button.

- **Port monitoring**: Generally speaking, the **default ports** for **POP3 (110)**, **IMAP (143)** and **SMTP (25)** are monitored. If your system's port settings are different than these, you can customise this accordingly.

Web/IM

You can create the following settings here.

Internet content (HTTP)

- **Process Internet content (HTTP)**: In the web options, you can determine that all ***HTTP web content*** is checked for viruses whilst browsing. Infected web content is not run at all and the corresponding pages are not displayed. To set this option, please check **Process Internet content (HTTP)**.

> If the network is using a proxy to access the Internet, the server port the proxy is using must be entered. Otherwise monitoring Internet traffic will not be possible. Web content monitoring (available in G Data EndpointProtection) also uses these settings.

- **Avoid browser timeout**: Since G Data software processes web content before it is displayed in the Internet 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 Internet browser because the browser does not receive data immediately due to the antivirus software checking it for malicious routines. This error message can be suppressed by setting the checkmark next to **Avoid browser timeout**. As soon as all browser data is checked for viruses, these will then be transmitted to the Internet browser.

- **Download size limit**: With this function you can interrupt the HTTP check 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 downloading large files.

- **Global whitelist for web protection**: This function allows you to generally exempt certain web sites from the web protection check.

Instant Messaging

- **Process IM content**: Since viruses and other malware can also be spread via Instant Messaging, G Data software can also prevent infected data from being displayed and downloaded in advance. If the Instant Messaging applications do not run using standard ports, please enter the corresponding ports under **Server port(s)**.

- **Instant Messaging (integration into IM application)**: If you use **Microsoft Messenger (version 4.7 and later)** or **Trillian (version 3.0 and later)**, you can set the checkmark for the respective program to make a context menu available in which you can directly check suspicious files for viruses.

> If you do not want to check the Internet content, the **Virus monitor** engages if you access infected downloaded files. That means that the system on the respective client is also protected without checking Internet content as long as the virus monitor is active.

AntiSpam

You can create the following settings here.

Spam filter

If you set the checkmark next to **Use spam filter** client email traffic will be checked for possible spam mails. As soon as an email is identified as spam or falls under suspicion of being spam, you can define a warning that will be displayed in the subject line of the email.

> You or the user can define a rule on the client in the mail program where, for example, mail that has **[Spam]** in the subject line will automatically be moved to a special folder for spam and junk mail.

Exchange settings

This chapter concerns the main settings required for operating G Data MailSecurity. This task area is only available if the G Data plug-in for Microsoft Exchange 2007 / 2010 has been installed. At the top of this tab are the following buttons:

This function updates the view and loads the current client settings from the G Data AntiVirus ManagementServer.

Updates the virus database on the G Data MailSecurity client with files from the G Data AntiVirus ManagementServer.

Switches on **automatic updates for the virus database**. Clients periodically check whether updated virus signatures are available on the G Data AntiVirus ManagementServer and run an automatic update.

Updates the program files on the client. The client program files held on the G Data AntiVirus ManagementServer are used. A client reboot may be necessary after updating the program files.

Switches on automatic updates for program files. The G Data MailSecurity plug-in periodically checks whether a new version of the G Data AntiVirus ManagementServer exists and automatically runs an update.

General

The email traffic check mentioned above is activated by default. If the check mark next to the **On-access scan** is removed, the automatic virus scan for email is also disabled. It is expressly not recommended that you disable this automatic scan.

As in the G Data client software for workstations, G Data MailSecurity has an idle scan and automatically runs a scan when the CPU load is low. With G Data MailSecurity, all objects in the Microsoft Information Store are checked for viruses by the idle scan. The idle scan can be configured to only run at specific times of the day. This is done by enabling **Only run idle scan within the following time frame**; entering the times you want ensures that the full computing power is available for other purposes outside of the times you have entered. This means for example that the idle scan can be configured so that it only runs in the evening or at night, outside of business hours. If the computer is not used at the weekend, for example, checking the box next to **Run idle scan all day on weekends (Sat., Sun.)** restricts the check to the weekend. The **Perform idle scan only on files that have been modified after a certain time** option gives the system administrator the option of only checking objects that do not exceed a specific age in days.

Scan settings

- **Use engines**: The G Data software works with two independently operating virus analysis units. In principle, you must use both engines to guarantee optimum virus combat results. However, using a single engine does have performance benefits – analysis can be performed more quickly if only one engine is used. We recommend the setting **Both engines - performance optimised**. In this scenario, both virus scanners cooperate such that optimised detection accuracy is achieved within a minimised scanning duration.

- **In case of an infection**: Here you can specify what is supposed to happen if an infected message is discovered. By setting **Move file to quarantine**, an infected message is moved to a special directory that is created by the G Data AntiVirus ManagementServer. Infected messages are encrypted there so that possible malware can no longer be executed. Messages in **quarantine** can be disinfected by the network administrator, deleted, moved back to their original storage location or, if required, sent to the **Internet clinic** .

- **Infected archive**: Specify here how infected **archives** are to be treated. When specifying these settings, you should bear in mind that a virus in an archive will only be harmful when it is unpacked from the archive.

- **File types**: Here you can define the file types G Data should check for viruses. Bear in mind that a check of all objects of the information store, depending on their size and the available computing power, can take a certain amount of time.

  Heuristics: Heuristic analysis detects viruses not only on the basis of constantly updated virus databases, but also based on detecting characteristics that are typical of most viruses. The heuristics can generate a false alarm in rare instances.

  Archive: Checking compressed data in archives is a very time-consuming process and can generally be omitted if the G Data AntiVirus Client is installed and enabled on your system. The monitor can detect a previously hidden virus while the archive is being unzipped and can automatically prevent it from spreading. Nevertheless, during regular checks of the computer outside the actual usage times, checking of the archives should also take place.

Status

For every Exchange server that is protected by G Data MailSecurity, there will be a display indicating which version of the G Data software is installed, which version the virus signatures have and when the last time was that the client reported to the G Data AntiVirus ManagementServer. Here you can check whether the clients are running properly and whether the virus signatures are up-to-date.

The following information is available in a list:

- **Computer**: The name of the Exchange server is identified here.
- **Engine A / Engine B**: Version number of the virus database.
- **Database**: The data and time when the status of the virus database of G Data MailSecurity was updated. This date is not identical with the update date of the virus database.
- **G Data Client version**: Here you will find the version number and the creation date of the G Data Client software being used.
- **Last access**: This entry shows you when G Data MailSecurity had a connection to the G Data AntiVirus ManagementServer.

- **Virus signature update / time**: Here you can determine whether the update to the most current virus database is completed, whether a job has been issued to carry this out or whether there were irregularities or errors.
- **Program update / time**: If new updates of G Data MailSecurity were imported, you receive the corresponding status information here.

The columns can be sorted according to different criteria by simply clicking on the corresponding column name. The column according to which current sorting is carried out, is indicated by a small arrow symbol.

Reports

All virus results, PolicyManager reports (where G Data EndpointProtection has been installed) and all firewall reports (with G Data ClientSecurity or EndpointProtection) are displayed in this task area. The status of the report will be displayed in the first column of the list (e.g. **Virus detected** or **Moved file to quarantine**). If a virus is found, you can respond by selecting the entries in the list and subsequently selecting a command from the context menu (right mouse button) or from the toolbar. Thus, for example, infected files can be deleted or moved in the **Quarantine folder** .

In the **Reports** task area, all reports appear under the name given to them and can be sorted according to different criteria by simply clicking on the respective column name. The column according to which current sorting is carried out, is indicated by a small arrow symbol. The following criteria are available:

- **Status**: You receive a short and concise display of the content of the respective report here. Informative icons underscore the importance and type of the respective report.
- **Computer**: The computer from which the respective report is made is displayed here. All computers are listed individually with user groups.
- **Date/time**: The date on which the report is created, based either on an acute virus result through the G Data monitor or on the basis of a scan job.
- **Reporter**: This entry can be used to inform you of whether the report is generated by the **virus scanner** as the result of a scan job, automatically through the **monitor**, or via the G Data email plug-in.
- **Virus**: if known, the name of the virus detected is displayed here.
- **File / Mail / Content**: The file in which a virus is found or in which a suspected virus exists is listed here. For **email**, you will also find the email address of the sender listed here.

- **Directory:** Directory information for the file concerned is important in case a file is quarantined and is subsequently to be moved back again.
- **User:** User who was logged in when the virus was discovered.

In the menu bar, an additional menu entry is available for the task area **reports**. For functions that operate with files (delete, move back, etc.), you must select the respective file or files in the report overview. You can select the following functions here.

- **View**: Indicate whether you would like to see all reports, only reports with viruses not removed or only quarantine reports here. You can also view the quarantine content.
- **Hide dependent reports**: If, due to different jobs or jobs that were performed multiple times, a virus alert or a report is displayed twice or more, you can hide the duplicate using this option. Only the most current entry is then shown and can be edited.
- **Hide archived files**: Here you can hide or show messages about reports from archive checks. If a virus is detected in an archive, the G Data software generally issues two messages, the first of which tells you that an archive is infected and the second of which tells you precisely which file in THIS archive is affected. These two messages are combined.

If you have set up the **scan jobs** on your system so that these simply log viruses found, you can also execute the virus countermeasures manually. To do this, select one or more logged file(s) in the report and then run the desired operation:

- **Remove virus from the file**: Attempts to remove the virus from the original file.
- **Move file to quarantine**: Moves the file to the **quarantine** folder.
- **Delete file**: Deletes the original file on the client.
- **Quarantine: Clean and move back**: An attempt is made to remove the virus from the file. If this succeeds, the cleaned file is moved back to its original location on the respective client. If the virus cannot be removed, the file is not moved back.
- **Quarantine: Move back**: Moves the file from the quarantine folder back to the client. **Warning**: The file is restored to its original state and is still infected.

- **Quarantine: Send to Internet Ambulance**: If you discover a new virus or an unknown phenomenon, always send us this file via the quarantine function in the G Data software. We will analyse the virus and send you a countermeasure as quickly as possible. Naturally our **Emergency AntiVirus service** will handle the data you sent with the utmost confidentiality and discretion.
- **Delete**: Deletes the selected reports. If reports to which a quarantine file belongs are to be deleted, you must confirm the deletion once more. In this case, the files found in quarantine are also deleted.
- **Delete dependent reports**: If a virus alert or a report is displayed twice or more due to different tasks or tasks being performed multiple times, you can delete the duplicate entry from the log file using this option.

Update

This function updates the view and loads the current **reports** from the G Data AntiVirus ManagementServer.

Delete reports

This function deletes the selected reports. If reports to which a **Quarantine** file belongs are to be deleted, you must confirm the deletion once more. In this case, the files found in quarantine are also deleted.

Print

Use this function to start the print procedure for reports. In the selection screen that appears, you can specify which details and areas you would like to print.

Page view

Using the page preview function you can obtain a preview of the page to be printed on the monitor before actually printing it out.

Remove virus

Using this function you can attempt to remove the virus manually from the original file. The success or otherwise of this attempt is indicated in the overview.

Move to quarantine

This function moves the selected files into the quarantine folder. The files are encrypted and saved in the **quarantine** folder on the G Data AntiVirus ManagementServer. The original files are deleted. The encryption ensures that the virus cannot cause any damage. Please ensure that for each quarantined file there is a corresponding report. If you delete the report the quarantined file is also deleted. You can send a file from the quarantine folder for examination by the **Emergency AntiVirus service**. For this, open the context menu of a quarantine report with a right-click.

In the report dialog, click the **OK** button after entering the submission reason.

Delete file

With the function **Delete file**, you delete the original file on the client.

Move back file from quarantine

Moves the file from the **quarantine** folder back to the original location on the client.

Warning: The file is restored to its original state and is still infected.

Clean file and move back out of quarantine

The virus is removed from the file with this function and the cleaned file is moved back to the client. If the virus cannot be removed, the file remains in the **quarantine** folder.

Show options

With a large number of different reports, it is useful to show and list these according to particular criteria. The following options are available:

Hide dependent reports: If, due to different jobs or jobs that were performed multiple times, a virus alert or a report is displayed twice or more, you can hide the duplicate using this option. Only the most current entry is then shown and can be edited.

Hide archived files

Hide read reports

Show all reports

Show all reports with unremoved viruses

Show all quarantine reports

Show quarantine contents

Show all HTTP reports

Show all firewall reports (in case you are using a software version with firewall)

Show all application control reports (in case you are using a software version with application control)

Show all device control reports (in case you are using a software version with device control)

Show all web content control reports (in case you are using a software version with web content control)

Clients

In the **Client selection area** select a group to obtain an overview of all the clients in the group. The version of the installed client, the version of the virus signatures and the last time the client reported to the G Data AntiVirus ManagementServer will be displayed for each client. This enables you to check whether the clients are running normally and if the virus signatures are fully up to date.

In the **clients** task area, the following information is available in a list. It can be sorted according to different criteria by simply clicking on the corresponding column name. The column according to which current sorting is carried out, is indicated by a small arrow symbol. The following criteria are available:

- **Computer**: The name of the client is displayed here.
- **Engine A / Engine B**: Version number of the virus database.
- **Database**: The date and time at which the status of the virus database was updated on the client. This date is not identical with the update date of the virus database.
- **G Data Client version**: here you will find the version number and the creation date of the G Data Client software being used.
- **Last access**: This entry lets you know when the G Data Client connected to the G Data AntiVirus ManagementServer.
- **Virus signature update / time**: Here you can determine whether the update to the most current virus database is completed, whether a job has been issued to carry this out or whether there were irregularities or errors.
- **Program update / time**: If new updates to the client software occur, you receive the corresponding status information here.
- **Exception directories**: If you have created exception directories that are not to be incorporated in the virus monitoring, the corresponding **Existing exceptions** are displayed here.

- **Subnet server:** This displays which subnet server the G Data AntiVirus Client is allocated to.

In the menu bar, an additional menu entry named **Client settings** is available with the following functions for the task area **Clients**:

- **Install G Data Client**: Installs the client software. Installation is only possible if the clients meet certain requirements (see **Install G Data Client**).
- **Install G Data Client for Linux**: You can also install special client software on Linux clients in the network. For more information, see the section **Installation of the client software on Linux computers** in the annex of this documentation.
- **Uninstall G Data Client**: Commands the G Data Client to uninstall itself. For a complete removal, the client computer must be restarted. The user is prompted to do this by a message (see also **Uninstall G Data Client).**
- **Reset to default**: To protect the entire network or selected groups, you can create **group settings** and thereby quickly issue standardised specifications for virus protection. In order to reset individual rules for single groups back to the general state, you can use this function to reset the group settings to the globally defined default values.
- **Move G Data Client to group**: This function allows the network administrator to move the selected client to an existing group. By selecting this function, all existing groups are displayed in their own window. To move a client to a group, select the relevant group and click on **OK**.
- **Assign G Data subnet server**: While you have the option of assigning specific ***subnet servers*** to clients with the function **Manage server** , you can also select a subnet server targeted for the respective client via the function **Assign G Data subnet server**.
- **Update virus database now**: Updates the virus databases on the clients with the files from the G Data AntiVirus ManagementServer.
- **Automatically update virus database**: Enables automatic updating of the virus database. Clients periodically check whether

an updated virus database is available on the G Data AntiVirus ManagementServer and run an automatic update.

- **Update program files now**: Updates the program files on the clients with the files from the G Data AntiVirus ManagementServer. A client reboot may be necessary after updating the program files.
- **Automatically update program files**: Switches automatic updating of program files on. Clients periodically check whether a new client program version is available on the G Data AntiVirus ManagementServer and run an automatic update.
- **Restart after update of program files**: As network administrator, you can specify here what priority an update of the program files has on the clients. Thus you can use **Open message box on client** to inform a user that he should restart his client computer at a convenient time, via **Create report** using the log files in the area **Reports**, or via **Perform restart without querying** automatically force a restart.

Using the buttons located above, you can decide whether you want to edit a general **Overview** of the clients or whether you want to send individual client **Messages**. By sending these messages you can quickly and conveniently inform users of this client about changes to its status.

Overview

From here you obtain an overview of all the managed clients and can also simultaneously carry out any client administration.

Update

This function updates the view and loads the current client settings from the G Data AntiVirus ManagementServer.

Delete

You can remove a client from the **Client view** here.

Print

Use this function to start the print procedure for the client list. In the selection screen that appears, you can specify which details and areas of the clients you would like to print.

Page view

Here you can, prior to the actual print out, output a preview of the page to be printed to the monitor.

Install G Data Client

1 **Port 7161 (TCP)** must be enabled on the server to enable the clients to connect to it.

2 To ensure communication from the server to the client, **port 7167 (TCP)** must be enabled on the client.

3 Where a firewall is used, an **exception** for the **gdmms.exe** file must be defined in it.

4 In a Windows workgroup, **Simple File Sharing** (in Windows XP) or the **Use Sharing Wizard** option (in Windows Vista or Windows 7) must be disabled. In addition the User Account Control (UAC) must be disabled.

5 Access to the C$ and Admin$ shares on the client is required.

6 A **password** must be allocated. An empty password field is not permitted.

7 The **Remote Registration Service** must be enabled in the **Services**.

Activating this function opens a dialogue window in which you enter access data for the server to be used for installing the G Data Clients.

After entering the relevant data (which is saved by the program so it does not need to be re-entered every time), please confirm by clicking **OK**. A dialogue box then opens in which all available clients are displayed. Select one or more disabled clients here, then click on **Install**. The G Data software then automatically installs the client software on the relevant computers. If the software cannot be installed using the **remote installation** described here, you can also install it on the client manually or with the **client installation package**.

To be able to access **disabled clients**, they must be displayed as enabled in the client list. When the **Install G Data Client** function is being used, the software informs you of this as necessary and allows the disabled clients to be displayed.

You can also install special client software for **Linux clients**. For more information, see the section **Installation of the client software on Linux computers** in the annex of this documentation.

Following successful client installation the client computer needs to be restarted.

If you are using a software version with a firewall: When installing the client software, you will be asked if the **G Data Firewall** should also be installed on the client computer. Further information on the **firewall** is available in the section of the same name in this documentation.

Uninstall G Data Client

Commands the G Data Client to uninstall itself. For complete removal the client must be restarted. The user is prompted to do this by a message.

Alternatively it is also possible to uninstall the client locally using the command line. This requires a prompt with administrator rights. In the **C:\Program Files(x86)\G DATA\AVKClient** directory, enter the command

```
UnClient /AVKUninst
```

to start the uninstall. A reboot may be required. If such a request does not appear, the computer must be restarted within max. 10 minutes.

Update virus database

Updates the virus database on the client with the files held on the G Data AntiVirus ManagementServer.

Automatically update virus database

Enables **automatic updating of the virus database**. Clients periodically check whether updated virus signatures are available on the G Data AntiVirus ManagementServer and run an automatic update.

Update program files

Updates the program files on the client. The client program files held on the G Data AntiVirus ManagementServer are used. A client reboot may be necessary after updating the program files.

Automatically update program files

Enables automatic updating of program files. Clients periodically check whether a new version is available on the G Data AntiVirus ManagementServer and execute an automatic update.

Process directory exceptions

You can define client directory exceptions here that are not to be checked during the execution of scan jobs.

Note that system variables and wildcards cannot be used here.

Messages

As a network administrator you can send **Messages** to individual clients or client groups. By sending these messages you can quickly and conveniently inform users of this client about changes to its status. The messages are displayed as an information message on the bottom right of the desktop of the client computer.

To create another message, simply click on the **New** button. In the dialogue which now appears, you can either select or deselect the clients you want to send the message to. Now type your information in the **Message** field for the clients concerned and click the **Send** button.

If you want a message to be accessible only to certain users of a client computer or network, then please enter their login names under **User name**.

PolicyManager

The PolicyManager includes application, device and web content control as well as monitoring of the Internet usage time. These functions allow comprehensive implementation of company guidelines for the use of internal company PCs. One can thereby determine via the PolicyManager whether and to what extent external mass storage or visual media can be used. Similarly, one can also define which websites may be visited within which time period and which programs may be used on the company PCs.

The **Settings** button makes a selection of various message options available. If the respective checkmarks are set here, the user has the option via a tray dialog on the respective client computer to request approval for a resource from the network administrator. If the checkmarks are not set, these options will not be available to the respective user.

Application control

Application control can be used to restrict specific programs for use by selected clients. To do this, under **Status** specify whether the limitations should apply to all users of the client in question or only to users who do not have administrator rights on the client computer. Under Mode, you can now specify whether the application control list should be a whitelist or a blacklist.

- **Whitelist**: Only the applications listed here can be used by the client computer.
- **Blacklist**: Applications listed here cannot be used on the client computer.

Creating new rules

A new rule can be defined via the **New...** button. The rule types **Vendor**, **File** and **Directory** are available for selection.

- **Manufacturer**: Here the manufacturer information contained in program files can be used to allow or block use of these applications. You can either enter the vendor's name here yourself or select a specific file via the **Find vendor...** button, from which the manufacturer information can be read and imported.
- **File**: Here you can block or allow specific program files for the particular client. To do this, you can either enter the file name to generally forbid or allow access to files with this name or click on the button **Determine file properties...** to define a file in a quite specific manner based on its properties. If necessary you can use an asterisk (*) as a placeholder at the start and/or end of the file name, product name and copyright properties.
- **Directory**: Using this function you can enable or block complete directories for clients (if necessary including their subdirectories).

Device control

Device control can be used to restrict access to external storage media. This means that USB sticks can be prevented from being used, and use of CD/DVD drives with write or read authorities and use of cameras can be restricted.

> Under **Status** you can specify whether the limitations should apply to all users of the client in question or only to users who do not have administrator rights on the client computer.

The device classes for which use can be restricted for each client are displayed under **Device**. These do not necessarily have to be present on each client. You can, for example, generally forbid the use of floppy disks for selected user groups, regardless of whether any particular computer has a floppy drive or not.

The following permissions can be defined:

Read / write: Full access to the device is allowed.

Read: Media can only be read; saving data is not permitted.

Deny access: Both read and write access to the device are not permitted. The device cannot be accessed by the user.

Whitelist

By use of the whitelist settings you can again allow access for a client user, with certain limitations, to devices to which you had previously limited access in some way or another (**Read** / **Deny access**). If you click on the **New...** button, a dialogue window opens in which devices with usage limitations are displayed. If you then click on **[...]**, you can permit exceptions for certain devices.

- **Use medium ID**: For example, here you can specify that only certain CDs or DVDs can be used with a CD/DVD drive, such as special company presentations on CD.
- **Use hardware ID**: For example, here you can specify that only certain USB sticks may be used. With releases based on hardware-ID for individual storage devices, the network administrator has the option to control which employees have the option to transmit data.

To determine a medium-ID or hardware-ID, click the **Client** entry in the dialogue box **Read hardware ID / medium-ID** and select the client on which the medium or hardware to be enabled is located. The corresponding ID is then read automatically.

Using the local search, you can read the ID of the medium or the hardware with the aid of the computer on which the G Data AntiVirus ManagementServer is installed. For this, the medium must be connected to the corresponding machine or inserted there.

Web content control

Web content control is used to provide users with Internet access within the scope of their duties but to prevent surfing of non-desirable websites or in particular subject areas. After selection of the client to be edited on the right side of the program interface, you can select or block certain areas by checking or unchecking a checkbox for the client in question.

The categories for this cover a large number of subject areas and are constantly updated by G Data. Network administrator costs associated with maintaining white- and blacklists thus no longer apply.

Under **Status**, you can specify whether the limitations should apply to all users of the client in question or only to users who do not have administrator rights on the client computer.

Global whitelist...

Using the **Global whitelist**, and regardless of any settings that have been made under Allowed categories**, it is possible to ensure that certain websites are blocked company-wide across the entire network. For example this may be the website of your own company. To do this, simply enter the address which you would like to enable under URLs**, then click on the **Add** button and the corresponding site is enabled.

Global blacklist...

Using the **Global blacklist**, and regardless of any settings that have been made under **Allowed categories**, it is possible to ensure that certain websites are blocked company-wide across the entire network. To do this, simply enter the address which you would like to block under **URLs**, then click on the **Add** button to block the corresponding site.

Internet usage time

In the **Internet usage time** area, general use of the Internet can be restricted to certain times. Setting up a time quota for Internet usage is also possible. Under **Status** you can specify whether the limitations should apply to all users of the client in question or only to users who do not have administrator rights on the client computer. On the right side, you can use the available scroll bar to specify the quota available for Internet usage on the client in question. Daily, weekly or monthly quotas can be issued; for example, the specification **04/20:05** corresponds to an Internet usage time of 4 days, 20 hours and 5 minutes.

> 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, then the software will automatically limit Internet usage to four days.

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

The **Lock out times** field allows you to, in addition to limiting Internet usage times, block particular time periods. 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, 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.

G Data Firewall

In this area you can centrally administer the firewall for the relevant clients or groups. **Overview** gives the system administrator an overview of the current status of the firewall on the installed clients; **Rule sets** offers options for creating and managing rule sets.

Overview

All client computers or clients in a selected group are displayed in the overview. This enables you to see at a glance which settings the client firewall concerned has and to make changes directly by clicking on the client concerned.

> **Rule set or Autopilot?**
> There are two fundamentally different options for operating a firewall.
>
> - **Autopilot**: When the firewall is running on "Autopilot", it is preconfigured by default by **G Data** and carries out its tasks in the background, without interrupting the user with queries. In Autopilot mode, the firewall optimises its rule sets autonomously over time.
> - **Rule set**: As administrator you can also define individual firewall rules for different computers.

The display list contains the following data:

- **Computer**: Client computer name. You can use the icons being displayed to tell if the client software is installed on this client.
- **Firewall**: Here you can tell if the firewall on the client is enabled, disabled or not even installed.
- **Autopilot / Rule set**: You can allocate different firewall modes to different clients (see above).
- **Offsite configuration**: If you select a client for offsite configuration, the user can manage and configure the firewall settings on this client how he wants, as long as he is not connected to the G Data AntiVirus ManagementServer network. The offsite configuration can only be used if the Firewall in the company network is not being operated in autopilot mode.

To change the firewall settings for the clients selected in the list, right-click on the entry. This will open a selection menu with the following options:

- **Create rule set**: This allows you to switch to the **Rule sets** area and define specific rules for your client firewall.
- **Edit rule set**: This takes you to the **Rule sets** area where you can modify existing rules for your client firewall.
- **Install Firewall**: You can use this function to install a firewall centrally on enabled client computers and subsequently administer them.
- **Uninstall Firewall**: This function is used to uninstall the current client firewall.

Firewall settings

Enable Firewall: By checking this box, the firewall on the client concerned is enabled. If you uncheck the box, the firewall is disabled.

- **Report blocked applications**: If this box is checked and the client computer is connected to the G Data AntiVirus ManagementServer, the system administrator will be notified in the **Reports** area of applications that have been blocked by the relevant client firewall.

- **User can enable/disable the firewall**: As network administrator, here you can allow the user of the client computer to temporarily disable the firewall. This option is only available if the client is inside the company network and should of course only be enabled for competent users.

- **Use offsite configuration for mobile clients**: In the **offsite configuration**, firewall rule sets for the client computer that apply to your company network can be created using default rule sets that automatically control the way that the Internet and networks that are secure, unsecure or should be blocked are handled. This enables mobile computers to be optimally protected whenever they are outside of the G Data AntiVirus ManagementServer network. As soon as the mobile computer is reconnected to the G Data AntiVirus ManagementServer network, these default rule sets are automatically replaced by rule sets that apply to that particular client within your network.

- **The user can change the offsite configuration**: This option will allow competent users to configure their firewall how they want outside of the network. As soon as the mobile computer is reconnected to the G Data AntiVirus ManagementServer, the changes made will be replaced with the rules put in place by the network administrator for this client.

The **offsite configuration** can only be used if the Firewall in the company network is not being operated in **autopilot mode**. If a client in the company network uses autopilot settings for the firewall, the autopilot settings can also be used when the client is not connected to the network.

Rule sets

In the **Rule sets** area you can set up custom firewall rules for all your network's requirements and areas. You can find detailed information on how to set up, administer and use rules in the documentation on using the firewall.

Statistics

In this task area, you can permit the display of statistical information about virus occurrences and client infections. Various views are available: the data can be displayed in text format or shown graphically (column or pie chart). The relevant view can be selected under **Display mode**. It contains data on the status of the **clients**, the **detection method** and the **virus hit list**. Select the relevant are in the display to view the data.

G Data AntiVirus Client

The **client software** provides virus protection for the clients and runs the G Data AntiVirus ManagementServer jobs allocated to it in the background without a separate user interface. The clients possess their own virus signatures and their own scheduler, so that virus analyses can also be run in offline mode (e.g. for notebooks that do not have a continuous connection to the G Data AntiVirus ManagementServer).

Installation of the clients

If installation of the clients over the network should fail, you can install the client software directly on the client computers. Check the **Remote installation requirements** beforehand. To install the client on a client computer locally, please place the G Data DVD in the client computer's DVD drive and press the **Install** button. Then select the **G Data AntiVirus Client** component by clicking on the adjoining button. During installation, enter the **server name** or the **IP address of the server** on which the G Data AntiVirus ManagementServer is installed. The server name is required so that the client can communicate with the server over the network. Furthermore, you must enter the **computer name** for this computer if this is not automatically displayed.

To install clients for Samba file servers, please read the following section in the annex of this documentation: **Installation of the client for Samba file server.**

Tray icon

After the installation of the client software, a display tray icon is available to the user of the client so that he can also check his system for viruses independently of administrative specifications. Approval of this option by the system administrator is required for this.

Using the right mouse button, he can click on the G Data Client icon to open a context menu which contains the following options:

Virus check

With this option, the user can also carry out a targeted check on his computer using the G Data AntiVirus Client, even outside of the virus checking period specified in the G Data Administrator. The user can also check floppy disks, CDs/DVDs, the memory and Autostart area, and individual files or directories. In this way, notebook users who only rarely connect their computers to the company network can prevent a virus attack in a targeted manner. In addition, he now has the option of moving virus-infected files to a local quarantine folder, thus making them harmless and available to the network administrator for further appraisal at the next opportunity.

> The user can also easily check files or directories from Windows Explorer by selecting the files or directories and using the **Check for viruses (G Data AntiVirus)** option in the context menu with the right mouse button.

During an ongoing virus check, the context menu is expanded with the following entries:

- **Virus check priority**: The user has the option of determining the priority of the virus check here. With **High**, the virus check is carried out quickly, although it can significantly slow down work with other programs on this computer. With the **Low** setting on the other hand, the virus check takes a comparatively long time, but other work on the client computer is not significantly slowed.
- **Stop virus check**: This option enables the user to stop a locally started virus check himself. Scan jobs that are defined by the G Data AntiVirus ManagementServer can only be stopped if the job administrator has enabled the **User can halt or cancel the scan job** option when setting up the job.
- **Cancel virus check**: This option enables the user to cancel a locally started virus check himself. Scan jobs that are defined by the G Data AntiVirus ManagementServer can only be cancelled if the job administrator has enabled the **User can halt or cancel the scan job** option when setting up the job.
- **Display scan window**: With this option, the user can display the information window in which the course and progress of the virus check is displayed. This option is only available if a virus check has been launched locally.

Disable monitor

Using this command, the G Data Monitor can be switched off by the user for a specified time (from **5 minutes** up to **until the next computer restart**). This is only possible if the system administrator has assigned the corresponding rights. For example, the temporary switching off of the monitor may be useful during extensive file copying procedures as this would considerably speed the process up. Real-time virus checking is also switched off during this interval.

Options

As long as the G Data administrator has enabled the option **The user can change email and monitor options**, the user can adjust the client options for virus checking on his computer as well as the options for the monitor which runs in the background to meet his own requirements.

> **Warning**: In this way, all protection mechanisms of the G Data software can be disabled on the client. This option should only be accessible to technically experienced users.
>
> The security-relevant settings under **Options...** can also be password-protected. Accordingly the administrator assigns the relevant client an individual password, with which the user can change the virus control functions on the client. This password is granted via the work area **Settings** in the G Data Administrator under **Password protection for changes to options** .

The individual setting options that are available to the user in the area **Options** are explained in detail in the area **G Data Administrator program setup > Task areas > Settings** in the following sections:

- **Monitor**
- **Email**
- **Virus check**
- **Web/IM filter**
- **Spam filter**

If you enable the option **The user can run virus checks** for the user on his client, he can check his client computer for viruses independently of the scan jobs specified in the G Data AntiVirus ManagementServer. The settings that are possible here for the user on the client correspond to the greatest possible extent to those found in the **Monitor** application.

Quarantine

Every client has a local quarantine folder into which infected files (depending on the settings for the monitor/scan job) can be moved. A file that was moved into quarantine cannot execute any malware if it contains a virus. Infected files are automatically zipped and encrypted when they are moved to quarantine. For quarantining certain files that are larger than 1 MB, they are always automatically stored in the local client quarantine so that the network is not needlessly burdened in case of a massive virus attack. All files that are smaller than 1 MB are transferred to the quarantine folder of the G Data AntiVirus ManagementServer. These settings cannot be changed. If an infected file that is less than 1 MB is detected on a mobile client without a connection to the G Data AntiVirus ManagementServer, it is saved in the local quarantine and only transferred to the quarantine there during the next contact with the G Data AntiVirus ManagementServer. Infected files can be disinfected in the quarantine folder. If this doesn't work, the files can be deleted from there and, if necessary, moved back to their original location from the quarantine.

Warning: Moving back does not remove the virus. You should only select this option if the program cannot run without the infected file and you nevertheless need it for data recovery.

The **client quarantine** is located in the directory

C:\ProgramData\G DATA\AntiVirusKit Client\Quarantine

The **G Data AntiVirus ManagementServer quarantine** is located in the directory

C:\ProgramData\G DATA\AntiVirus ManagementServer\Quarantine

Internet update

The G Data AntiVirus Client can also be used to carry out independent Internet virus signature updates from the client computer if no connection to the G Data AntiVirus ManagementServer is available. This option can also be enabled for individual clients by the network administrator.

> Use the **Settings and scheduling** button to run scheduled virus signature updates on the client.

Firewall

Users can make extensive changes to their client firewall settings in the Firewall area, if this option has been switched on at the server for the client concerned. As long as the client is in the G Data AntiVirus ManagementServer network, the firewall can be administered centrally from the server. The **Firewall** option is only available if the G Data Administrator has given the client permission to modify the firewall settings. For more detailed information on configuring and using the firewall see: **Firewall settings**.

About

About can be used to find out the version of the installed G Data software and virus signatures.

G Data WebAdministrator

The **G Data WebAdministrator** is web-based administration software for the G Data AntiVirus ManagementServer. It can be used to create settings for the G Data AntiVirus ManagementServer via a web interface in a browser.

Installation of the G Data WebAdministrator

When installing the G Data WebAdministrator, you may be asked to install **Microsoft .NET Framework components**. These are essential for operating the G Data WebAdministrator. After the installation you will need to restart the computer.

Warning: BEFORE installing the G Data WebAdministrator you need to enable the **IIS Metabase and IIS 6 configuration compatibility** Windows function. If this function is not available, installation of the G Data WebAdministrator will be cancelled. This setting can be found, for example, in Windows Vista under **Start > Control panel> Programs > Programs and Functions > Switch Windows Functions on or off**. You can switch the setting on or off here in **Internet Information Services > Web Management Tools > IIS 6 Management Compatibility > IIS Metabase and IIS 6 configuration compatibility**. Furthermore the **www services** must also be enabled, if this has not already been done. To do this, please check the box in **Internet Information Services > World Wide Web Services**.
In the server operating systems, one can find the corresponding options in the server manager in **Roles**.

The G Data WebAdministrator requires Microsoft Silverlight. If this is not available when installing the software, you will be notified of this during the first start of the G Data WebAdministrator. A subsequent installation of Silverlight is possible.

You can now install the G Data WebAdministrator.

After the installation you will see the icon for the **G Data WebAdministrator** on the desktop of your computer.

G Data WebAdministrator program setup

To use the **G Data WebAdministrator**, click on the G Data WebAdministrator desktop icon. Your web browser will then open automatically at a login page for accessing the G Data WebAdministrator. As with your usual **G Data Administrator** enter your **Access data** then click on the **Log in** button. In operation and functionality, the G Data WebAdministrator corresponds to the **G Data Administrator**.

G Data 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 are sent. 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. It is generally advisable to use the firewall in **Autopilot mode**. It then runs in the background and protects the system without the user having to undertake settings.

> If you are using the firewall in **Autopilot mode**, this will remain completely in the background and operate independently. If you are using the firewall with **user-defined**settings, a dialogue window will appear in the event of doubt in which you can gradually optimise the firewall for your system environment. Autopilot mode is included as standard when installing the firewall.

You can use the **Settings** and **Edit...** buttons to choose between Autopilot mode and Create rules manually for the firewall.

Configure

The following options are only available locally on the client if the client is in offsite mode. The item **Firewall...** is then accessible via the context menu of the client. Changes to the firewall settings should only be made accessible to experienced users as changes there can have far-reaching consequences to the security of a system.

Status

In the Status area of the firewall, the user obtains information about the current status of the firewall. By double-clicking the relevant entry (or by selecting the entry and clicking the **Edit...** button), you can directly select actions here or switch to the relevant program area.

- **Security**: The firewall gradually learns which programs are used for accessing the Internet and which programs present a potential security risk. Depending on the need, the firewall can be configured so that it either provides very good basic protection without posing many enquiries or professional protection, which is geared towards very precise computer usage habits. This type of configuration, however, requires knowledge on the part of the user. Double-click on **Security** to call up a range of security versions:

  Autopilot mode: Here the firewall works fully autonomously and automatically keeps threats from the PC. This setting offers practical all-around protection and is recommended in most cases.

  Manual rule creation: If the firewall is configured individually or if particular applications do not work together with the autopilot mode, the user can gear the firewall protection completely to his needs.

- **Mode**: Basic setting of the firewall. The options here are either **Automatic (autopilot)** or **Create rules manually**
- **Networks**: The firewall monitors all activities of the networks with which the computer is connected, such as a **DTN network** and a **LAN connection**. If one or more networks are not protected, for example, because they were manually excluded from firewall monitoring, a warning icon will alert you about this. Double-clicking the respective entry opens a dialogue box via which the user can individually configure the rules and settings for the selected network.

  The **Direct Internet connection** setting is, for the most part, based on the settings that also apply to **Trustworthy networks**.

  Each **network** can be assigned a special **rule set**. Whilst the **Networks** area tells you which networks are available on your computer, the **Rule sets** area tells you which automatically created or user-defined rule sets are available in the firewall.

- **Registered attacks**: As soon as the firewall registers an attack on the computer, it will be displayed here. Further information is available by double-clicking.
- **Application radar**: The application radar displays which programs are currently being blocked by the firewall. If a blocked program is given permission to use the network after all, it is selected and approved via the **Allow** button.

Networks

The Networks area lists the networks (e.g. **LAN**, **data transmission network** etc.) to which the computer is connected. Also shown here is which **rule set** (see section **Rule sets**) is assigned to the respective network. The firewall can also be disabled for particular networks by removing the checkmark in front of the respective network. Disabling the firewall is only recommended if there is a justifiable interest in doing so (e.g. diagnostics). The firewall settings for a network can be viewed or modified by connecting to the network and subsequently clicking the **Edit...** button.

Edit network

When processing network settings, the user can choose between the **Rule wizard** or **extended edit mode.** We generally recommend using the rule wizard since it helps the user create rules and settings.

- **About network**: This is where you can find information about the network - where this is available - concerning 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 determine whether all computers connected via a **TCP/IP network** should have access to the Internet or not. This **Internet connection sharing** (**ICS**) can generally be activated for home networks.
- **Enable automatic configuration (DHCP)**: A **dynamic IP-Address** is issued when connecting your computer with the network. 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. Rule sets specified by the network administrator or issued by oneself are accessible. Clicking the **Edit rule set** button gives you the option of configuring rule sets individually. For more information see the section entitled **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 a **direct connection to the Internet**, **untrustworthy networks**, **trustworthy networks**, and **networks to blocked.** The relevant rule set is listed with names and stealth mode status in the overview. You can change existing rule sets or add new ones using the **New...**, **Delete...**, and **Edit...** buttons.

> **Stealth mode** hidden, unnoticeable) is used for not answering requests to the computer that verify the relevant port's accessibility. This makes it difficult for attackers to obtain system information in this manner.
>
> 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). Protection of networks of various threat levels is possible. The firewall contains three default rule sets for the following network types:

- **Rule set for an untrustworthy network**: This generally covers open networks (e.g. **data transmission networks**) with **Internet** access.
- **Rule set for a trustworthy network**: **Home and company networks** are generally trustworthy.

- **Rule set for a network to be blocked**: 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 **external networks** with an indeterminate level of security (e.g. external corporate networks, public workspaces for notebooks etc.)

If a connection to a new network is established, the corresponding rule set can be assigned depending on the threat level. Creating a rule set for a network is also possible. To do this, click the **New...** button in the **Rule sets** area and enter the following details in the dialogue 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 basic default rules for untrustworthy, trustworthy networks or for networks to be blocked. You can then make individual adjustments based on these defaults.

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**). Clicking on **Edit...** opens the **Rule wizard.** Depending on the need, the user can also change to the **extended edit mode** for editing the individual rules of this rule set. You can learn how to define new rules in the rule sets in the sections entitled **Using the Rule wizard** and **Extended edit 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** .

Rule wizard

The Rule wizard allows you to define specific additional rules to the relevant rule set or modify existing rules.

> Using the Rule wizard you 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 actions are available in the Rule wizard:

- **Allow or deny access to a specific application**: You can hereby select a targeted application and permit or prohibit access to the network as part of the selected rule set. Simply use the wizard to select the desired program **(program path)**, then indicate under **Connection direction** whether the program is to be blocked for incoming connections, outgoing connections or both incoming and outgoing 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).
- **Open or disable a specific Internet service (port)**: The wizard provides the option of blocking ports completely or enabling them for a particular application only (e.g. CRM software).
- **Allow or deny file and printer sharing (NetBIOS)**: **NetBIOS** is a special interface in networks that can be used for e.g. sharing files or printers directly between one computer and another without using the TCP/IP protocol. It is often advisable to deny sharing for untrustworthy networks, as this is generally not necessary for home networks and the NetBIOS can also be used by attackers to compromise a computer.
- **Allow or deny domain services**: Enabling for domain services in untrustworthy networks should generally be denied.

- **Enable Internet connection sharing**: If your system connects directly to the Internet you can determine whether all computers connected via a **TCP/IP network** should have access to the Internet or not. This **Internet connection sharing** (**ICS**) can generally be activated for home networks.
- **Switch to the extended edit mode**: This allows you to move from the Rule wizard to the **extended edit mode**. For further information, see the section **Extended edit mode**.

> If you remove the checkmark next to **Always launch the Rule wizard in the future** checkbox, the firewall will automatically open the advanced dialogue to define new rules.

Extended edit mode

An experienced user can define individual rules for the respective network here. The rules that are created here can also be created through the Rules wizard. Moreover, the following options are available:

- **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, unnoticeable) is used for not answering requests to the computer that verify the relevant port's accessibility. This makes it more difficult for attackers to obtain information about the system.
- **Action if no rule applies**: Here, you can specify if access to the network should generally be permitted, denied, or subject to an inquiry. Should any special rules for individual programs be defined by the firewall's **learning function**, these will naturally be applied.
- **Adaptive mode**: 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 **extended edit mode** via the **New...** button
- Using the dialogue 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 partly nested hierarchically, it is sometimes important to note the **ranking** 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 dialogue** or modify an existing rule using the **Edit dialogue**, the **Edit rule** dialogue appears with the following setting options:

- **Name**: For default and automatically generated rules, this displays the **program name** to which the relevant rule applies. You can also use the **Edit...** button at any time to change the name or add further information.
- **Rule enabled**: You can disable a rule without actually deleting it by deactivating the checkbox.
- **Remark**: This indicates how the rule was created. **Default rule** is listed next to rules preset for the rule set; **generated in response to alert** is listed next to rules that arise from the dialogue from the **Firewall alarm**; and for rules that you generate yourself via the advanced dialogue you can insert your own comment.
- **Direction of connection**: With **Direction**, you specify if the selected rule applies to incoming or outgoing connections, or to both incoming and outgoing 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 universally block or enable protocols or link use of a protocol to 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 address space**: 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.

Firewall alarm

When in **Create rules manually** 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 the user details about the relevant application. The user also has the option here of allowing one-off or permanent access to the network, or denying any access. As soon as you have allowed or denied permanent access for a program, a **rule** will be created in that network's **rule set** regarding this and you will not be asked about it again.

The following buttons are available:

- **Always permit**: This button lets you create a rule for the application mentioned above (e.g. **Opera.exe**, **Explorer.exe** or **iTunes.exe**) granting the application in the named network permanent access to the network and/or Internet. 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 mentioned above that permanently denies the application in the named network access to the network and/or Internet. You will also find this rule as a "Rule created by inquiry" in the **Rule sets** area.
- **Block this time**: You can use this button to ban the relevant application from accessing the network only once. 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.

Log

The Log area logs all the connections permitted or blocked by the firewall. You can sort this list as desired using different criteria by clicking on the relevant column header. Click the **Details...** button for further information on the individual connections.

Options - firewall

In the upper menu bar of the program interface, you will find comprehensive functions and setting options by clicking the **Settings** button.

Automatic

There are two different modes available here:

Autopilot mode (recommended): Here the firewall works fully autonomously and automatically keeps threats from the PC. This setting offers practical all-around protection and is recommended in most cases.

Manual rule creation: If the firewalls need to be configured individually, or certain applications do not work with the autopilot mode, the firewall rules can be set entirely according to your requirements.

Attachment

Troubleshooting (FAQ)

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

I have installed the G Data software without registering it. How can I register the software?

To register the software post-installation, open the **Internet update** under Start > All Programs > G Data > G Data AntiVirus ManagementServer. There you will find the **Online registration** option. Clicking on this button opens the registration form. Enter the registration number for the product here. Depending on the type of product, you can find this in the licence document (MediaPack) or order confirmation. In case of doubt contact your dealer or the relevant distributor.

> On entering the registration number your product is enabled. The access data generated is displayed following successful registration. **Be sure to make a note of this access data!** Following successful registration it is no longer possible to re-enter the licence key. If you have problems entering your registration number, please check if you have entered it correctly. Depending on the font used, a capital "I" (for India) is often misread as the number "1" or the letter "l" (for Lima). The same applies to: "B" and "8", "G" and "6", "Z" and "2".
>
> If you have purchased G Data ClientSecurity or G Data EndpointProtection and did not activate it on installation, the **Firewall** and **PolicyManager** tabs are only enabled following successful activation. Until then only the G Data AntiVirus Business functions are available.

I want to execute client installation centrally from the server via the G Data Administrator

The most convenient way is to **run the installation via the G Data Administrator**. However, to do this, the clients must meet certain prerequisites:

1. **Port 7161 (TCP)** must be enabled on the server to enable the clients to connect to it.

2. To ensure communication from the server to the client, **port 7167 (TCP)** must be enabled on the client.

3. Where a firewall is used, an **exception** for the **gdmms.exe** file must be defined in it.

4. In a Windows workgroup, **Simple File Sharing** (in Windows XP) or the **Use Sharing Wizard** option (in Windows Vista or Windows 7) must be disabled. In addition the User Account Control (UAC) must be disabled.

5. Access to the C$ and Admin$ shares on the client is required.

6. A **password** must be allocated. An empty password field is not permitted.

7. The **Remote Registration Service** must be enabled in the **Services**.

Remote installation can be completed in two ways. If the client meets the necessary prerequisites, the files are copied directly and entries made in the registry. If the server can only access the hard drive and not the registry, or if other system prerequisites are not met, the entire set-up program is copied to the client and started automatically at the next computer reboot. To install, simply access the G Data Administrator menu bar and choose the **Clients > Install G Data Client** function. An input window appears in which you should enter the user name, password and domain for the G Data AntiVirus ManagementServer. After this data is entered a window appears showing all available network computers. Enabled clients are marked as such with an icon. Disabled clients are represented by a greyed-out icon. Select a network computer for installation and click on the **Install** button. The G Data AntiVirus Client is then installed on this computer. If your system does not meet the prerequisites for remote installation of the G Data Client software, you of course have the option of using the G Data Client software to install clients manually or semi-automatically.

I want to install the G Data Administrator on a client computer

You can of course start the **G Data Administrator** from any other computer in the network as well.

> It is not necessary to install the G Data Administrator on the connected client computers for this to work smoothly.
>
> Installing the G Data Administrator on a client computer is recommended if on-site access to the G Data AntiVirus ManagementServer settings is required.

We recommend that the **Admin** directory is shared and then invoking the **Admin.exe** file from the other computer. Of course you can also copy the file to another computer and launch it from there. Sharing has the advantage that you are always launching the latest version, as the file can be updated via Internet update. Optionally you can also place the G Data DVD in the DVD drive of the client computer, press the **Install** button then select the G Data Administrator component by clicking the corresponding button. In the following start screen, you are informed that you are about to install the G Data Administrator on your system. Please ensure that you have now closed all open applications in your Windows system, as otherwise they may cause problems during the installation. Click on **Next** to continue with the installation. The next screen allows you to select the location where the G Data Administrator data is to be saved. By default the G Data Administrator is saved under **C:\Program Files\G DATA\G DATA AntiVirus ManagementServer\Admin**. If you want to select a different storage location, you can use the **Browse** button to open a directory view where you can select or create a new directory. **Next** takes you to the next installation step. Now you can select a program group. If you click on **Next**, you will usually see the program in the **G Data\G Data Administrator** program group in the Windows start menu program selection screen. The installation ends with a completion screen. Click on **Exit**. You can now use the G Data Administrator. The administrator tool for managing the G Data AntiVirus ManagementServer is accessed by clicking on the **G Data Administrator** option in the **Start > (All) Programs > G Data > G Data Administrator** program group in the Start menu.

Error message "You must have at least Microsoft Exchange Server 2007 SP1"

If you receive the error message listed below, the minimum requirements for installing G Data MailSecurity have not been fulfilled. For an installation, Microsoft Exchange 2007 with Service Pack 1 is the minimum requirement. This must be installed BEFORE G Data MailSecurity. For this, see also **Installation** and **System requirements**.

I want to configure the clients using the G Data CD-ROM with the client software

You can also install the client software directly on individual clients using the supplied DVD. Place the DVD in the DVD drive of the client computer, then select the **G Data AntiVirus Client** component by clicking on the button next to it. During the installation you will be asked for the name of the computer on which the G Data AntiVirus ManagementServer is installed. Enter the corresponding name (e.g. **avk_server**). Click on the **Next** button to complete the installation. If the setup program asks for a computer restart on the completion screen, please do so as the client will only become functional after a restart.

Some clients report that "The virus database is corrupt". What can be done?

In order to ensure optimal virus protection, the integrity of the virus database is regularly checked. If an error occurs, the report **The virus database is corrupt** is included. Delete the report and download the current update of the virus database from our server. Subsequently perform an update of the virus database on the affected clients. Please contact our telephone hotline if the error report is included again.

The MMS should only be addressed via its IP address, not its name.

Installing the G Data AntiVirus ManagementServer: The server name will be requested during the installation. The name must be replaced by the **IP address**. You can also replace the server name later through the IP address if the G Data AntiVirus ManagementServer has already been installed. To do this alter the registry entry

HKEY_LOCAL_MACHINE\SOFTWARE\G DATA\AVK ManagementServer\ComputerName

and

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\G DATA\AVK ManagementServer\ComputerName

accordingly.

Enabling the clients in the G Data Administrator: In order that the connection from the server to the clients can also be established via the IP address, the clients must be enabled in the G Data Administrator with their IP address. This can be done either manually (**enable clients/client (dialog)**) or by searching an IP address space (**search for client/computer**). **G Data Client setup from the DVD**: If the clients are installed directly from the DVD, the installation program asks for both the server name and the name of the computer. Enter the appropriate IP address here.

My mailbox was moved to the quarantine.

This can happen if an infected email is found in the mailbox. **Move file back** : Close the mail program on the affected client and delete any possibly newly created archive file. Then use the G Data Administrator to open the associated report and click on **Move file back**. Please contact our support if moving back fails.

How can I check whether the clients have a connection to the G Data AntiVirus ManagementServer?

The **Last access** column in the **Clients** task area contains the date on which the client last reported to the G Data AntiVirus ManagementServer. In the default setting the clients report to the G Data AntiVirus ManagementServer every five minutes (if there are no scan jobs currently running). The following reasons may cause a failed connection:

- The client is disabled or disconnected from the network.
- A TCP/IP connection cannot be established between the client and the G Data AntiVirus ManagementServer. Check the network settings.
- The client cannot determine the IP address of the server, i.e., the name resolution is not functioning. The connection can be tested using the **telnet** command at the prompt. **Port 7161** must be accessible on the **server** and port **7167** must be accessible on the **client**. Check the connection using the **telnet <SERVERNAME> <PORTNUMBER> command**

> Note that under **Windows Vista, Windows 7** and **Server 2008 (R2)** the telnet command is not available by default. Therefore enable the relevant Windows function or add it to the server as a new feature. If the connection from the client to the server is intact, an array of cryptic characters appears in the prompt:

If the connection from the server to the client is intact, an empty input window appears:

Some clients report that "Program files were changed or are corrupt". What can be done?

In order to ensure optimum virus protection, the integrity of the program files is regularly checked. If an error occurs, the report **Program files were changed or are corrupt** is included. Delete the report and download the current update of the program files (G Data Client) from our server. Subsequently perform an update of the program files on the affected clients. Please contact our telephone hotline if the error report is included again.

Storage locations and paths

G Data AntiVirus Client virus signatures:

- XP / Server 2003 / Server 2003 R2: C:\Program Files\Common Files\G DATA\AVKScanP\AVAST5 or BD
- Vista / Win7 / Server 2008 / Server 2008 R2: C:\Program Files (x86)\Common Files\G DATA\AVKScanP\AVAST5 or BD

G Data AntiVirus ManagementServer virus signatures:

- XP / Server 2003 / Server 2003 R2: C:\Documents and Settings\All Users\Application Data\G DATA\AntiVirus ManagementServer\Updates
- Vista / Win7 / Server 2008 / Server 2008 R2: C:\ProgramData\G DATA\AntiVirus ManagementServer\Updates

G Data AntiVirus Client quarantine:

- XP / Server 2003 / Server 2003 R2: C:\Program Files\Common Files\G DATA\AVKScanP\QBase
- Vista / Win7 / Server 2008 / Server 2008 R2: C:\Program Files (x86)\Common Files\G DATA\AVKScanP\QBase

G Data AntiVirus ManagementServer quarantine:

- XP / Server 2003 / Server 2003 R2: C:\Documents and Settings\All Users\Application Data\G DATA\AntiVirus ManagementServer\Quarantine

- Vista / Win7 / Server 2008 / Server 2008 R2: C:\ProgramData\G DATA\AntiVirus ManagementServer\Quarantine

MMS databases (integrated; only up to and including Version 10.7)

- XP / Server 2003 / Server 2003 R2: C:\Documents and Settings\All Users\Application Data\G DATA\AntiVirus ManagementServer\Database
- Vista / Win7 / Server 2008 / Server 2008 R2: C:\ProgramData\G DATA\AntiVirus ManagementServer\Database

MMS databases (SQL)

XP / Server 2003 / Server 2003 R2 / Vista / Win7 / Server 2008 / Server 2008 R2:

- C:\Program Files\Microsoft SQL Server\MSSQL.1 \MSSQL\Data\GDATA_AntiVirus_ManagementServer.mdf
- C:\Program Files\Microsoft SQL Server\MSSQL.1 \MSSQL\Data\GDATA_AntiVirus_ManagementServer_log.ldf

After client installation, some applications run significantly slower than before

The monitor oversees all file accesses in the background and checks the files there for viruses. This normally leads to a *delay* that is barely perceptible. If an application opens many files or opens some files very often, a significant delay can occur. To avoid this, first temporarily disable the monitor to find out whether the delays are being caused by it. If the affected computer accesses files on a server, you must also temporarily disable the monitor on the server. If the monitor is the cause, the problem can usually be remedied by defining an *exception* (= files that are not to be checked). For this purpose, the files that are frequently accessed must be identified. You can identify this data with a program such as *MonActivity*. If necessary, contact our **ServiceCenter**.

> Naturally you can also increase performance by using just one engine rather than two for virus checks. This primarily applies to older systems.

Installation of the client software on Linux computers

The product makes it possible to use **G Data virus protection** on **Linux workstations** of various distributions. The **Linux client** can thus (as with **Windows clients**) be linked into the G Data ManagementServer infrastructure, centrally managed via the G Data Administrator software and supplied with signature updates. As with Windows clients, a file system monitor with a graphical user interface will be set up with Linux clients that orients itself to the Windows version in terms of functionality. For Linux computers that operate as **file servers** and provide Windows authorisations to different clients (via the **SMB protocol**), a module can be installed manually. This controls access to the authorisations and carries out a file scan with every access event, so no malware can migrate from the Samba server to the Windows clients (or vice versa).

For the **Workstation client** a kernel version equal to or greater than 2.6.25 is required; for example, this is the case with Ubuntu 8.10, Debian 5.0, Suse Linux Enterprise Desktop 11, and other current distributions. Customisation is required in isolated cases with other distributions. The **file server client** can be used on all prevalent distributions.

To install the software on the Linux client, proceed as follows:

1. **Remote installation of the client software via the network**
   In the **Clients** task area in the **Client settings** menu, select the command **Install G Data Client for Linux** . A dialogue window appears through which you can define the client on which the client software is to be copied. For this, the computer must be recognised in the network.

2. Use the selection **computer name** if a **Samba service** is installed on the client computer or if the computer is registered in the network's **name server**. If the name of the computer is not known, use the **IP address** of the computer.

3. Now enter the computer's **root password**. A root password must be allocated for a remote installation. By default, this is not the case with certain distributions, for example, Ubuntu.

4. Now click on the **Install** button. In the **Status** area, you can see if the installation of the client software was successful.

Manual installation of the client software

The following files can be found in the directory \Setup\LinuxClient on the program DVD:

- **installer.bin** = installer for the Linux client
- **uninstaller.sh** = uninstaller for the Linux client

You can copy these files to the client computer and start the corresponding file to install the client software.

In addition, you will also find a file here with the **virus signatures**. The installation of this file is optional since the software automatically obtains the latest virus signatures from the server after the installation:

- **signatures.tar** = Archive with virus signatures

Linux file server clients: No connection with the G Data AntiVirus ManagementServer has been made / signatures will not be updated

1 Check whether both G Data Linux Client processes are running: Enter the following in terminal

```
linux:~# ps ax|grep av
```

. You should receive the following

```
...        Ssl    0:07 /usr/sbin/avkserver --daemon
...        Ssl    0:05 /usr/sbin/avclient --daemon
```

You can start the processes regardless of the distribution used with

```
linux:~# /etc/init.d/avkserver   start
linux:~# /etc/init.d/avclient    start
```

and stop them with

```
linux:~# /etc/init.d/avkserver   stop
linux:~# /etc/init.d/avclient    stop
```

. To do this you must be logged in as the administrator (="root") on the Linux computer.

2 To view the log files see: In **/var/log/**, you will find the log file **gdata_install.log**. The remote installation process is logged in this file. In the **/var/log/gdata** directory, the log file **avkclient.log** can be found. In this log file, the scan results of the scanner **avkserver** and the output of the process **avclient** are logged, which establishes the connection to the G Data AntiVirus ManagementServer. Look at the files and search for any error messages. If you wish to see more messages, then you can set the entries for **LogLevel** to value **7**in the configuration files **/etc/gdata/gdav.ini** and **etc/gdata/avclient.cfg**.

Attention: A high LogLevel generates a lot of messages and causes the log files to quickly increase in size. Under normal operating conditions, always set the LogLevel to a low value!

3 Test the scanner: use the **avkclient** command line tool to test the functioning of the **avkserver** scan server. The following commands can be executed:

linux:~$ avkclient avkversion - outputs the version and latest update date of the virus signatures

linux:~$ avkclient avkversion - outputs the version in short format

linux:~$ avkclient scan:<file> - scans the file **<file>** and outputs the result

4 Check the configuration file: The **etc/gdata/avclient.cfg** file is the configuration file for the remote client **avclient**. Check whether the address of the main management server (MainMMS) is entered correctly. If not, delete the incorrect entry and log on the Linux client via the G Data Administrator again or enter the address of the G Data ManagementServer directly.

5 Test your authorisations: virus protection for the Samba authorisations is enabled via the entry

vfs objects = gdvfs

in the Samba configuration file **/etc/samba/smb.conf**. If the entry is in section **[global]**, protection for all releases is enabled. If the line is in another section, the protection only applies to the corresponding release. You can comment out the line for test purposes (by entering a hash symbol "#" at the start of the line) to see whether access functions without virus protection. If not, please first search for the error in your Samba configuration.

6 Linux workstation monitor

Check whether the monitor process **avguard** is running:

linux:~# ps ax|grep avguard

The monitor requires the **redirfs** and **avflt** kernel modules. With **lsmod** you can check whether the modules are loaded: **lsmod|grep redirfs** and **lsmod| grep avflt**.

The modules must be compiled for the kernel used by you. This is taken care of by the **Dynamic Kernel Module System** (**DKMS**), which must be installed together with the matching kernel header packages for your distribution. If this is the case, DKMS compiles and installs the modules automatically. You will find the monitor **log file** under **/var/log/gdata/avguard.log**.

Index