Table of contents

G Data Business

In these days of global networking and the massive security risks it incurs, virus protection is no longer just for IT specialists. It has to be considered within the context of a comprehensive, company-wide risk management strategy at the highest level of management. Computer network downtime caused by malware strikes a company where it is most vulnerable. The result: downtime for business-critical systems, loss of data, and loss of important communication channels. Computer viruses can cause damage to a company that it can never recover from!

G Data provides high-end virus protection for your entire network. For many years, G Data products' leading security capabilities have been awarded excellent scores in numerous tests. G Data business software is based on central configuration and administration plus as much automation as possible. All clients, whether workstations, notebooks or file servers, are controlled centrally. Client processes run invisibly in the background and automatic Internet updates enable extremely fast reaction times in the event of a serious virus attack. Central control via G Data ManagementServer facilitates installation, configuration, updates, remote control, and automation for the entire network. This reduces system administration workload and saves time and money.

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

Your G Data Team

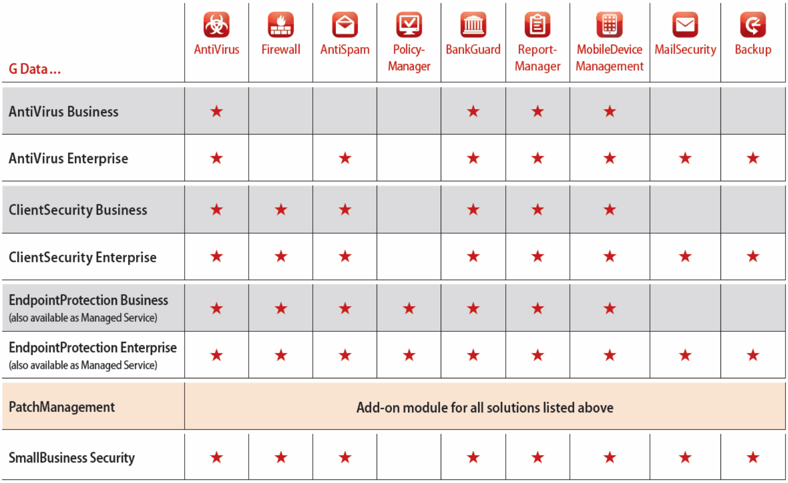
Software upgrades

This documentation describes the functionality of all available G Data business modules. In case you would like to use a module that is not included in your software version, contact **G Data Support** to obtain information about software upgrades.

Copyright

G Data Business solutions

G Data software products offer complete, comprehensive protection for end customers as well as medium- to large-sized enterprises. Thanks to the latest cutting-edge technology, our customers enjoy the highest possible level of security and the best performance coupled with ease of use. Our security modules are available as part of the following solutions:



G Data ...	AntiVirus	Firewall	AntiSpam	Policy-Manager	BankGuard	Report-Manager	MobileDevice Management	MailSecurity	Backup
AntiVirus Business	★				★	★	★		
AntiVirus Enterprise	★		★		★	★	★	★	★
ClientSecurity Business	★	★	★		★	★	★		
ClientSecurity Enterprise	★	★	★		★	★	★	★	★
EndpointProtection Business (also available as Managed Service)	★	★	★	★	★	★	★		
EndpointProtection Enterprise (also available as Managed Service)	★	★	★	★	★	★	★	★	★
PatchManagement	Add-on module for all solutions listed above								
SmallBusiness Security	★	★	★		★	★	★	★	★

Additional documentation

Extensive information about how to use G Data software can be found in the context-sensitive software help file, which can be opened at any time by pressing F1. Additionally, you can download a comprehensive manual in PDF format by visiting the G Data Support website:

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

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

International: **www.gdatasoftware.com**

Security Labs

If you discover a new virus or an unknown phenomenon, always send us the file via the Quarantine function. The function can be found in G Data Administrator under **Reports**. Right click on any reported file and choose **Quarantine: Send in to G Data Security Labs**. 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 confidentiality and discretion.

> The return address for responses from G Data Security Labs can be defined in G Data Administrator under **Options** > **Server settings** > **Email settings**.

Support

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**

The serial number can be found on the license certificate (if the product was obtained as MediaPack) or in the order confirmation. When in doubt, contact your reseller or distributor.

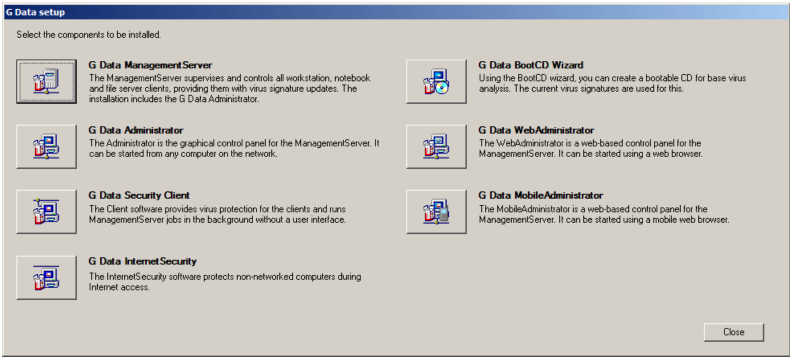
Before contacting the ServiceCenter, please check the configuration of your computer and network. The following information is of importance:

- The **version number** of G Data Administrator and G Data ManagementServer, which can be found in the **?**-menu of G Data Administrator
- The **serial number** or the Internet Update **username**
- The exact Windows version number (Client/Server)
- Additional hardware and software components (Client/Server)
- Any errors that may have occurred (error messages, including error codes) in their exact wording

By providing these details, contact with our Support staff will be easier, quicker and more successful. If possible, please make sure that you can readily access a pc on which G Data Administrator is available.

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 to avoid problems with files that need to be accessed by the G Data setup wizard. 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.



G Data setup

Select the components to be installed.

G Data ManagementServer
The ManagementServer supervises and controls all workstation, notebook and file server clients, providing them with virus signature updates. The installation includes the G Data Administrator.

G Data BootCD Wizard
Using the BootCD wizard, you can create a bootable CD for base virus analysis. The current virus signatures are used for this.

G Data Administrator
The Administrator is the graphical control panel for the ManagementServer. It can be started from any computer on the network.

G Data WebAdministrator
The WebAdministrator is a web-based control panel for the ManagementServer. It can be started using a web browser.

G Data Security Client
The Client software provides virus protection for the clients and runs ManagementServer jobs in the background without a user interface.

G Data MobileAdministrator
The MobileAdministrator is a web-based control panel for the ManagementServer. It can be started using a mobile web browser.

G Data InternetSecurity
The InternetSecurity software protects non-networked computers during Internet access.

- **G Data ManagementServer**: Install this component first. G Data ManagementServer will be used to manage all G Data-related settings and updates. G Data 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. When installing G Data ManagementServer, G Data Administrator is automatically installed on the same machine.

- **G Data Administrator**: G Data Administrator is the administration software for G Data ManagementServer and enables management of settings and updates for all G Data clients on the network. G Data Administrator is password-protected and can be installed on and launched from any Windows computer that has a network connection with G Data ManagementServer.

- **G Data Security Client**: The client software provides virus protection for the clients and runs the G Data ManagementServer jobs allocated to it in the background without the use of a separate user interface. Installing the client software is generally carried out through G Data Administrator for all clients.

- **G Data InternetSecurity**: When you are using a SmallBusiness solution, you can use G Data InternetSecurity as a self-sufficient security solution for computers that are not connected to your network (such as notebooks for field personnel). A complete manual for G Data InternetSecurity is included on the installation medium.

- **G Data MailSecurity**: G Data MailSecurity centrally secures all SMTP- and POP3-based email traffic. All Enterprise editions of G Data software include G Data MailSecurity, on a separate DVD.

- **G Data BootCD Wizard**: You can use the G Data BootCD wizard to create a bootable CD for basic scanning of your computer. This scan takes place before the operating system is launched and uses up-to-date virus signatures. The original G Data software DVD also functions as G Data BootCD.

- **G Data WebAdministrator**: G Data WebAdministrator is the web-based administration software for G Data ManagementServer. It can be used to create and edit settings for G Data ManagementServer through a web interface.

- **G Data MobileAdministrator**: G Data MobileAdministrator is a web-based control panel for G Data ManagementServer that is optimized for mobile devices. It can be launched from any mobile browser and offers access to the most important and frequently used functions of G Data Administrator. G Data MobileAdministrator is available for users of the AntiVirus, ClientSecurity, and EndpointProtection (Business/Enterprise) editions.

First steps

In the event of an acute virus threat, first run a **G Data boot scan** on the affected computers, before you proceed with the steps below.

1 Install **G Data ManagementServer** on your server. To guarantee optimal protection, the computer should always be accessible (switched on) and able to automatically download virus signatures via an Internet connection. To install G Data ManagementServer, a server operating system is not required (see **System Requirements**). While installing G Data ManagementServer, the wizard also installs **G Data Administrator**, the administration software for G Data ManagementServer.

2 Complete the online registration. Without online registration, no software or signature updates can be performed.

3 When G Data Administrator is first started on the server, the **Server Setup Wizard** is run. With it, **G Data Security Client** can be installed **remotely** on the desired clients in your network. All settings that are configured by the Server Setup Wizard can also be changed later.

> If problems arise with the remote installation of the clients, the client software can also be installed using **Active Directory synchronization**, or **locally** with the aid of the G Data DVD or a client install package. Client install packages can also be distributed using group policy objects/logon scripts. To ensure that the server is protected against virus attacks, installation of G Data Security Client is also recommended for the server.

4 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. G Data Administrator provides, among other things, options for real-time protection through 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, G Data Administrator can be installed **on every client** within the network. You use it to log in to G Data ManagementServer from any client. If it becomes necessary to resolve a critical situation from outside your network, **G Data WebAdministrator** can be used with every desktop web browser. With **G Data MobileAdministrator** you can even configure the software on the road using a mobile web browser.

System requirements

The following minimum system requirements apply to the G Data range of products:

Enterprise products and SmallBusiness Security

G Data ManagementServer/Security Client/MailSecurity (32-bit/64-bit)
Windows 8/Windows 7/Windows Vista/Windows XP SP3 (32-bit)
Windows Server 2012/Windows Server 2008/Windows Server 2003
with at least 1 GB available RAM.

Recommended system requirements for G Data ManagementServer:
Multicore CPU and at least 4 GB available RAM.

G Data MailSecurity (Microsoft Exchange plugin 64-bit)
Microsoft Exchange Server 2010/Microsoft Exchange Server 2007 SP1

Business products (without MailSecurity)

G Data ManagementServer/SecurityClient (32-bit/64-bit)
Windows 8/Windows 7/Windows Vista/Windows XP SP3 (32-bit)
Windows Server 2012/Windows Server 2008/Windows Server 2003
with at least 1 GB available RAM.

G Data products use the TCP/IP protocol for communication between the clients and the management server.

Port configuration

G Data products use several TCP ports for secure communication within the network. Make sure your firewall configuration allows traffic through the following ports:

Main server (MMS)

- Port 7161 (TCP): Communication with clients and subnet servers
- Port 7182 (TCP): Communication with G Data Administrator
- Port 7183 (TCP): Communication with mobile clients
- Port 7184 (TCP): Communication with mobile clients (distribution of mobile client installation files)

Subnet servers

- Port 7161 (TCP): Communication with clients and (subnet) servers

Clients

- Port 7167 (TCP): Communication with (subnet) servers
- Port 7169 (TCP): Communication with clients (peer-to-peer update distribution)

When you are using the Microsoft Exchange plugin of G Data MailSecurity MailGateway, make sure to configure port 7171 (TCP) on the machine where the plugin is installed to allow communication between the main server and the plugin.

Change ports

The port numbers have been chosen to minimise impact on existing software. However, if there happens to be a port conflict, you can change the port assignments for G Data ManagementServer. Firstly, open Services Control Manager (**Start**, **Run**, *services.msc*) with administrative privileges and stop the G Data ManagementServer background service. Navigate to the installation folder of your G Data product (typically C:\Program Files\G DATA\G DATA AntiVirus ManagementServer) and open the file *gdmms.exe.config* in a text editor like Notepad. Look for the following settings and change the ports number where necessary:

- **AdminPort**: Enter any port number. The default value is 0 (which sets the port to the standard number of 7182).

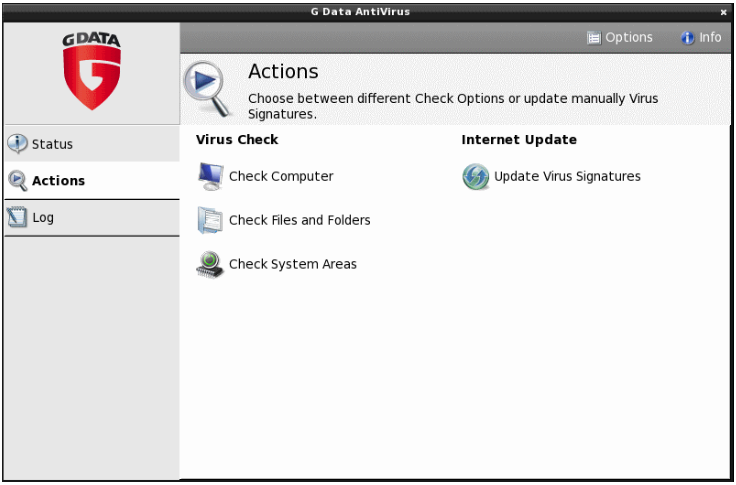
- **ClientHttpsPort**: The default value is 0 (which sets the port to the standard number of 7183). The ClientHttpsPort value should not be altered, as mobile clients do not accept an alternative port.
- **ClientHttpPort**: Enter any port number. The default value is 0 (which sets the port to the standard number of 7184).

When changing the value for ClientHttpPort or ClientHttpsPort, you have to reinitialise the HTTPS security configuration for the port. Open a command prompt with administrative privileges and run *C:\Program Files\G DATA\G DATA AntiVirus ManagementServer \gdmmsconfig.exe /installcert*.

After changing the ports, restart the G Data ManagementServer service. Note that, when changing the value for AdminPort, you will always have to specify the port when logging on to G Data Administrator, in the following format: *servername:port*.

G Data BootCD

Viruses that have embedded themselves on your computer may prevent G Data software from being installed. The G Data BootCD will help you fight these threats, prior to installation of antivirus software. G Data BootCD is run before the operating system is loaded.



Actions

Choose between different Check Options or update manually Virus Signatures.

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

1b **Using a G Data BootCD you have created yourself**: To create your own G Data BootCD, you must first install the G Data BootCD Wizard. The wizard must be run on a system on which a G Data Security Client with up-to-date signatures has been installed. After installing the G Data BootCD Wizard, **follow its on-screen instructions** to create the bootable G Data BootCD. Insert the CD into the drive.

2 Restart the computer. The G Data BootCD start menu will appear.

3 Use the arrow keys to choose the **G Data BootCD** option and confirm your choice with **Enter**. A Linux operating system is now started from the CD/DVD and the G Data BootCD interface appears.

> If you are having problems with the program interface display, restart your computer and choose the **G Data BootCD – alternative** option.

4 The program now suggests updating the virus signatures. Click **Yes** and perform the update. As soon as the signatures have been updated via the Internet, you will see the message **Update complete**. 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 still run the 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 BootCD yourself, the virus signatures are the latest ones that the G Data Security Client had available at the time the BootCD was created.

5 You will now see the program interface. Click **Check computer** 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 will once again be available.

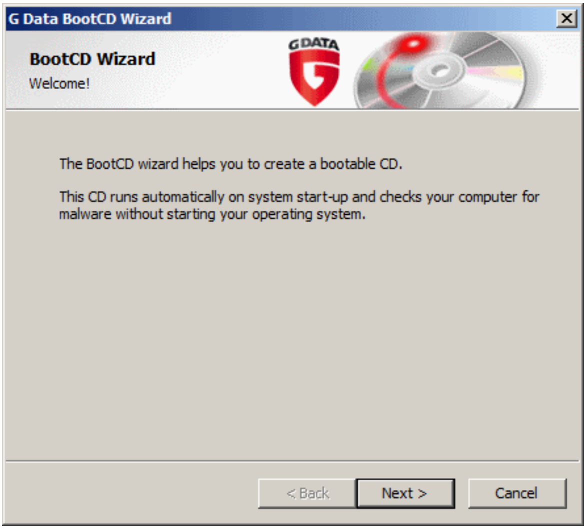
7 After completion of the virus check, click the **Exit** button (bottom right of the Linux program interface) then select **Restart**.

8 Remove the G Data BootCD from the drive.

9 Restart your computer. It will boot your default operating system. The G Data software can now be installed on a virus-free system.

Create G Data boot CD

To create your own G Data BootCD, you first have to install the G Data BootCD Wizard. This must be on a system on which a G Data Security Client with up-to-date signatures has been installed. Insert the G Data DVD and press the **Install** button. Then select **G Data BootCD Wizard** by clicking on the adjoining button.



G Data BootCD Wizard

BootCD Wizard

Welcome!

The BootCD wizard helps you to create a bootable CD.

This CD runs automatically on system start-up and checks your computer for malware without starting your operating system.

After finishing the installation, navigate to **Start** > **(All) Programs** > **G Data** > **G Data BootCD Wizard** and click **Create BootCD**. The wizard will lead you through the process of creating the G Data BootCD image. Make sure to let the wizard perform a virus signature update, in order to add the latest virus signature files to the boot CD image. After updating the signatures, the wizard offers to burn the boot CD directly to the selected target drive, or to save the CD as an ISO image. The ISO file can then be burned using external software, or distributed to network machines digitally.

Enable CD/DVD boot in BIOS

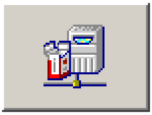
If your system will not boot from CD/DVD, you will need to enable this option in the BIOS, the motherboard firmware that is launched before your operating system. To make these changes, proceed as follows:

1 Shut down your computer and power off.

2 Start your computer. Usually you reach the BIOS setup by pressing the **DEL** key while the computer is booting up (sometimes the **F2** or **F10** key will work as well). The computer manufacturer's documentation will provide more information on this.

3. You can check your motherboard manufacturer's documentation for information on how to change settings in your BIOS setup. The result should be the boot sequence **CD/DVD-ROM**, **C:**, meaning that the CD/DVD-ROM drive becomes the **first boot device** and the hard disk partition with your Windows operating system on it becomes the **second boot device**.
4. Save the changes and restart your computer. Your computer is now ready for a boot scan.

Installing G Data ManagementServer



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

Ensure that you have closed all open applications, as they may cause conflicts during 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

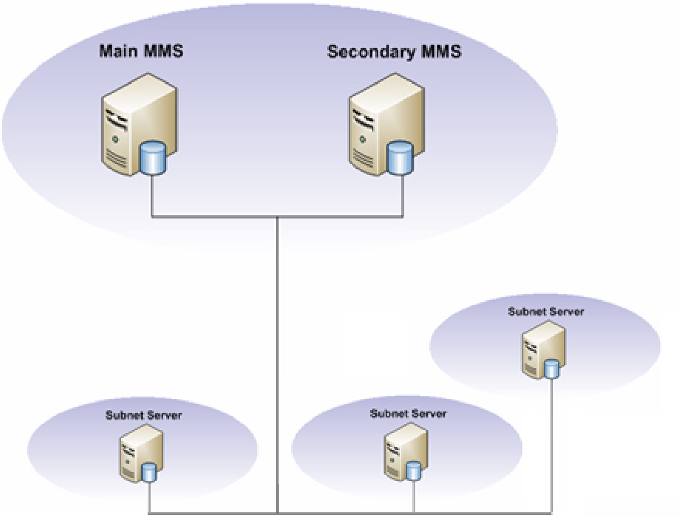
When selecting a server type you have the following options:

- **Install Main Server**: During an initial installation, G Data ManagementServer must always be installed as the main server (main MMS). The main server represents the central configuration and administration entity of G Data's network-based virus protection architecture. G Data ManagementServer provides the infrastructure for network clients to be protected with the latest virus signatures and program updates. In addition, all client configuration is managed centrally by G Data ManagementServer.
- **Install 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 more than one hour, 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 independently from one another to provide a safeguard against failure.

- **Install Subnet Server**: For large networks (e.g. company headquarters with connected branch offices) it can be sensible to operate an installation of G Data ManagementServer as a subnet server. Subnet servers help to reduce the network traffic load between clients and the main MMS. They can be used to manage a subset of 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 which ensures a safeguard against failure. Large networks can profit from using **peer to peer update distribution**. By enabling this option, server-client network traffic during updates is greatly reduced. For some networks this can eliminate the need of using a subnet server.



Database selection

Select the database G Data ManagementServer should use. You can choose between using **Microsoft SQL Express** and an existing **SQL Server instance**. A server operating system is not necessary. The SQL Server instance variant is primarily meant for use in larger networks with more than 1000 clients. The SQL Express variant is recommended for networks with less than 1000 clients.

Computer name

Check the **name** of the computer on which G Data ManagementServer is being installed. Network clients must be able to access the server by this name.

Product activation

Product activation occurs during installation. This enables immediate update downloads upon finishing the installation.

- **Enter Registration Number**: If you are installing 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 the registration number in the license document (MediaPack) or on the order confirmation. In case of doubt contact your G Data reseller or the relevant distributor. Upon entering the registration number, your product is activated. The access data generated (user name and password) are displayed immediately following successful registration. You will also receive an email containing these data. **Be sure to make a note of your user name and password and save the email!** Following successful registration, it is no longer necessary to re-enter the license key.

> If you have problems entering your registration number, verify that you have entered it correctly. 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 before, you will have received access data (user name & password) via email. To reinstall the G Data software, enter the access data here.

- **Activate Later**: If you just want to look over the software first or if the access data are temporarily unavailable, the installation can take place without entering the data. However, if you do so, no Internet updates will be downloaded. The G Data software can only effectively protect your computer if it is completely up-to-date. Using the software without activating it will protect you insufficiently. You can enter your registration number or access data subsequently at any time. See also the **notes on subsequent activation of the G Data software** in the FAQ section.

  > 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, G Data EndpointProtection, or any additional modules. The additional components are activated and available as soon as you register the software.

Database type configuration

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

Finalising installation

Following the installation of G Data ManagementServer, the G Data software is operational and ready to be configured. A server reboot may be required. G Data ManagementServer will automatically be started every time the system is booted up. 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 G Data ManagementServer.

Installing G Data Administrator

When installing **G Data ManagementServer**, G Data Administrator will also be automatically installed. Subsequent installation of the Administrator software on the server is not required. However, G Data Administrator can still be installed on any client computer. In this way, the G Data ManagementServer can also be serviced from any PC in the network.

To install G Data Administrator on a client computer, 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.

Ensure that you have closed all open applications, as they may cause conflicts during the installation. After clicking **Next**, the installation will continue; follow the installation steps with help of the installation wizard. After the installation, the entry **G Data Administrator** is available under **Start** > **(All) Programs** > **G Data** > **G Data Administrator**.

Installing G Data WebAdministrator

To install G Data WebAdministrator, place the G Data DVD in the client computer's DVD drive and press the **Install** button. Then select the **G Data WebAdministrator** component by clicking on the adjoining button.

The installation of G Data WebAdministrator is fairly straightforward. After accepting the license agreement, select a folder to install WebAdministrator to. It should be installed to the web server's HTTP folder (typically **\inetpub\wwwroot**).

During and after the installation, some extra software may need to be installed. WebAdministrator depends on the following prerequisites:

- *Microsoft Internet Information Services (IIS)*: As WebAdministrator is a web-based product, the server on which it will be installed should also be running a web server. WebAdministrator supports Microsoft Internet Information Services (IIS). Ensure you are running IIS before attempting to install MobileAdministrator.
- *IIS 6 Metabase Compatibility*: Before you install WebAdministrator, make sure that IIS 6 Metabase Compatibility is enabled on the IIS server. If it is not enabled, WebAdministrator cannot be installed. Under Windows 7, navigate to **Start** > **Control Panel** > **Programs and Features** > **Turn Windows features on or off**. Under **Internet Information Services (IIS)** > **Web Management Tools** > **IIS 6 Management Compatibility**, make sure **IIS Metabase and IIS 6 configuration compatibility** is selected. When using a Microsoft Server operating system, you will find a similar option on the **Roles** tab of **Server Manager**. Navigate to **Web Server (IIS)** > **Role Services** and make sure **IIS 6 Metabase Compatibility** is installed.
- *Microsoft .NET Framework*: WebAdministrator depends on the Microsoft .NET Framework. If the server does not yet have Microsoft .NET Framework installed, the installation wizard will prompt you to install it. After the installation, a reboot is required.
- *Microsoft Silverlight*: Running WebAdministrator requires the Silverlight browser plugin. If it has not been installed beforehand, the first time WebAdministrator is run you will be notified and offered a download link.

After the installation has finished, you will find an icon on your desktop to start **G Data WebAdministrator**. The installer will also provide you with a direct link to access WebAdministrator through your browser.

Using WebAdministrator over the Internet without using a secure connection represents a potential security risk. For optimal security, **enable an SSL Server Certificate in IIS**.

Installing G Data MobileAdministrator

To install G Data MobileAdministrator, place the G Data DVD in the client computer's DVD drive and press the **Install** button. Then select the **G Data MobileAdministrator** component by clicking on the adjoining button.

The installation of G Data MobileAdministrator is fairly straightforward, like its **WebAdministrator** counterpart. After accepting the license agreement, select a folder to install MobileAdministrator to. It should be installed to the web server's HTTP folder (such as **\inetpub\wwwroot**).

During the installation, some extra software may need to be installed. MobileAdministrator depends on the following prerequisites:

- *Microsoft Internet Information Services (IIS)*: As MobileAdministrator is a web-based product, the server on which it will be installed should also be running a web server. MobileAdministrator supports Microsoft Internet Information Services (IIS). Ensure you are running IIS before attempting to install MobileAdministrator.
- *Microsoft .NET Framework*: MobileAdministrator depends on the Microsoft .NET Framework. If the server does not yet have Microsoft .NET Framework installed, the installation wizard will prompt you to install it. After the installation, a reboot is required.

After the installation has finished, the installer will provide you with a direct link to access MobileAdministrator through your mobile browser.

Using MobileAdministrator over the Internet without using a secure connection represents a potential security risk. For optimal security, **enable an SSL Server Certificate in IIS**.

Installing G Data Security Client

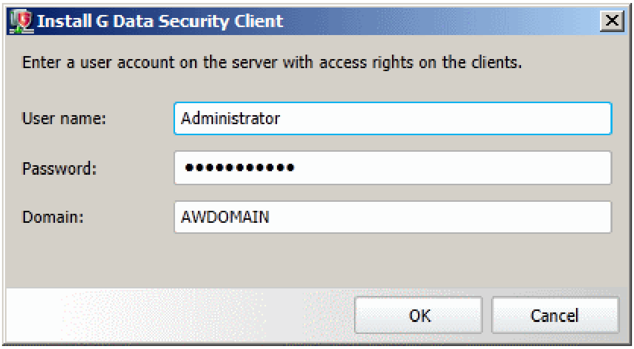
To protect and manage clients in the network, G Data Security Client needs to be installed on each machine. Depending on the deployment scenario, you can choose a **remote installation** (via G Data Administrator) or a **local installation** (using the G Data software DVD or a client install package). Additionally, it is recommended that you install G Data Security Client on your server.

Remote installation

The most convenient way to install clients is to initiate a remote installation through G Data Administrator. The **Server setup wizard** and the **Clients** module allow you to automatically install G Data Security Client to all machines.

In addition to the required **port configuration**, the machines must meet the following prerequisites:

- Where a firewall is used, an exception for gdmms.exe file must be defined in it.
- In a Windows Workgroup, Simple File Sharing (Windows XP) or the Use Sharing Wizard option (Windows Vista or Windows 7) must be disabled. In addition, User Account Control (UAC) must be disabled.
- Access to the C$ and Admin$ shares on the client is required.
- A password must be set. An empty password field is not permitted.
- The Remote Registration Service must be enabled in **Services**.



Install G Data Security Client

Enter a user account on the server with access rights on the clients.

User name: Administrator

Password: ●●●●●●●●●●●●

Domain: AWDOMAIN

Using the **Server setup wizard**, which is automatically run the first time you start G Data Administrator, you get an overview of all enabled computers in the network. You can also manually add and enable computers by name. Alternatively, the Clients module allows you to install G Data Security Client by selecting one or more machines in the client list, right-clicking on them and choosing **Install G Data Security Client**. After selecting the machines, both procedures carry on similarly. An input window appears in which you should enter the **user name**, **password** and **domain** with access rights on the clients. After selecting a display language for the client, you will be asked if **G Data Firewall** should be installed on the client PCs at the same time. The firewall is only available with G Data ClientSecurity, G Data EndpointProtection, and G Data SmallBusiness Security **solutions**. A dialog window will show the installation progress for all clients. Following successful client installation, the client computers need to be restarted.

> When using **Active Directory integration**, you can choose to automatically attempt to install G Data Security Client on newly added computers. The same prerequisites apply.

Remote installation can be completed in two ways. If the clients meet the necessary prerequisites, the files are copied directly and entries are 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 setup program is copied to the client and started automatically at the next computer reboot.

If your system does not meet the prerequisites for remote installation of the G Data Client software, or if remote installation fails, you can choose to install clients **locally** using the G Data software DVD or a client install package. A manually generated client install package can also be distributed using logon scripts/ group policy objects.

Local installation

If a **remote installation** is not possible, you can install G Data Security Client directly on the clients. You can use the G Data software DVD to manually install the client software, or create a client installation package that runs in the background (which makes it ideal for distribution through logon scripts).

G Data software DVD

Place the G Data DVD in the client computer's DVD drive and press the **Install** button. Select the **G Data Security Client** component by clicking on the adjoining button.

During installation, enter the **server name** or the **IP address of the server** on which G Data 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 it is not automatically displayed.

Client installation package

The package is a single executable file (GDClientPck.exe), which can be used to install a new client without any further user interaction. The installation package can be used to install the client to all computers in a domain via a login script, or to install locally, and it always contains the current client version available on the server.

To create an installation package, start G Data Administrator. In the menu **Organization**, click the option **Create G Data Security Client install package**. You will be prompted to select the ManagementServer with which the clients should register, and an installation language. After selecting a storage location, G Data Administrator will create an installation package in the background. The installation package can then be copied to the target computer and should be launched there with administrator rights. It will install G Data Security Client without further user interaction.

Installing Linux clients

Like their Windows counterparts, Linux clients can be linked with the G Data ManagementServer infrastructure, centrally managed via G Data Administrator and supplied with signature updates. As with Windows clients, a file system monitor with a graphical user interface will be set up on Linux clients, with functionality similar to the AntiVirus module for Windows. For Linux computers that operate as file servers and provide Windows authorization to different clients (via the SMB protocol), a module can be installed manually. This module controls access to the authorizations and carries out a file scan on every access, 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, included with distributions such as Ubuntu 8.10, Debian 5.0, Suse Linux Enterprise Desktop 11, and other vendor versions. Customization is required in isolated cases with some Linux versions. The file server client can be used on all prevalent versions of Linux.

Remote installation

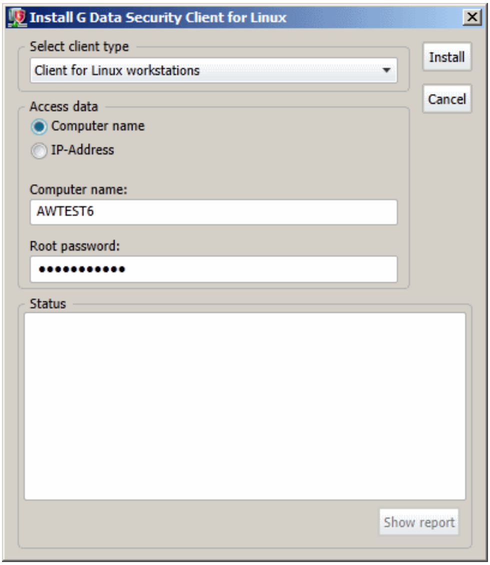
To remotely install the software on a Linux client, proceed as follows:

1. In the **Clients** module of G Data Administrator, open the **Clients** menu and select the command **Install G Data Client for Linux**. A dialogue window appears in which you can define the client that the software should be copied to. The computer must be recognized in the network.

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

3. Enter the computer's **root password**. A root password must be set in order to initiate a remote installation. Not all vendors set a root password by default (such as Ubuntu).

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



Install G Data Security Client for Linux

Select client type: Client for Linux workstations

Access data
● Computer name
○ IP-Address

Computer name: AWTEST6

Root password: ●●●●●●●●●●●●

Status

Local installation

The following files can be found in the directory \Setup\LinuxClient on the G Data 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 installer.bin to install the client software. In addition, the G Data DVD also features a file 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)

Installing G Data MailSecurity

Before beginning the installation, you should consider where in the network G Data MailSecurity will be installed. While you can use G Data MailSecurity Administrator from any point in the network, the installation of the G Data MailSecurity MailGateway component requires some planning. MailGateway should ideally be located directly behind your network firewall (if you are using one). That way, the SMTP/POP3 data stream from the Internet will be sent to MailGateway via the firewall and distributed from there.

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

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

Installation of MailGateway on the mail server (SMTP)

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

If you install G Data MailSecurity on the same computer as Microsoft Exchange 5.5, then the installation wizard will automatically change the port for incoming email. The SMTP entry in the *\winnt\system32\drivers\etc\services* file is changed and the Microsoft Exchange Internet mail service is restarted.

Sample configuration

Mail server configuration

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

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

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

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

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

Installation of MailGateway on a separate computer (SMTP)

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

1) Adjust the MX record in the DNS entry
2) Define redirection to the firewall (if available)
3) Change the IP address of the mail server and assign the computer with G Data MailSecurity MailGateway the original IP address of the mail server

Configuration

Mail server configuration

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

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

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

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

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

Installation wizard

Make sure to close all other programs before installing G Data MailSecurity to prevent file conflicts. Ensure that there is sufficient hard disk space for the installation. If there is insufficient space available, G Data MailSecurity will notify you.

The installation of G Data MailSecurity is straightforward. Place the G Data MailSecurity DVD in your DVD drive. An installation window opens automatically, offering the following options:

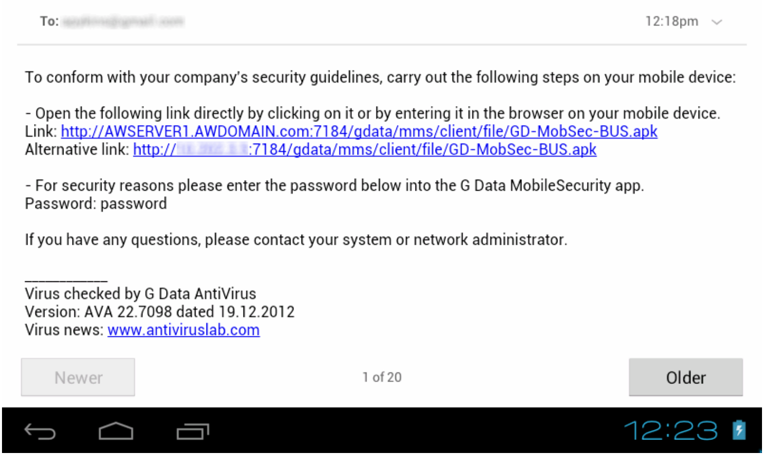
- **Install**: Installing G Data MailSecurity
- **Browse**: View the G Data MailSecurity DVD directories using Windows Explorer
- **Cancel**: Close the Autostart window without performing any actions

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

> If you choose to install the components for Statistical assessment, G Data MailSecurity Administrator's Status panel will show a Statistics button. It will allow you to view statistical information about the mail server and can be configured through **Options** > **Logging**.

Installing G Data MobileSecurity

To make use of G Data's Mobile Device Management capabilities, you can install a specially tailored business version of G Data MobileSecurity to your Android devices. G Data Administrator offers installation capabilities for mobile clients in its **client management area**. Click the icon **Send installation link to mobile clients** to send an e-mail containing a download link for the MobileSecurity app. You can enter multiple e-mail addresses, separated by line breaks or commas. If you have not entered a password yet in the **server settings**, enter it under **Authentication for mobile clients**.



To: [redacted]

To conform with your company's security guidelines, carry out the following steps on your mobile device:

- Open the following link directly by clicking on it or by entering it in the browser on your mobile device.
Link: http://AWSERVER1.AWDOMAIN.com:7184/gdata/mms/client/file/GD-MobSec-BUS.apk
Alternative link: http://[redacted]:7184/gdata/mms/client/file/GD-MobSec-BUS.apk

- For security reasons please enter the password below into the G Data MobileSecurity app.
Password: password

If you have any questions, please contact your system or network administrator.

____
Virus checked by G Data AntiVirus
Version: AVA 22.7098 dated 19.12.2012
Virus news: www.antiviruslab.com

Open the e-mail message on the mobile device and tap the download link to download the installer APK file. Note that the option **Unknown sources (Allow installation of non-Market apps)** needs to be enabled in order to install APK files. This option is usually found in Android's system menu **Settings** > **Security** > **Device Administration**.

After opening the APK file and confirming its requested permissions, G Data MobileSecurity will be installed and can be started from the Android app menu. Through the **Settings** icon in the top right corner of the screen, the app can be configured to allow remote administration. Tick the checkbox **Allow remote administration** and enter the name or IP address of the ManagementServer under **Server address**. Under **Device name** you can enter a name that will be used to identify the device in G Data Administrator. **Password** should contain the password that you entered in G Data Administrator (which is also listed in the installation e-mail).

The device will be listed among the other clients in G Data Administrator's **Clients** module and can be managed from there. If it does not appear automatically, reboot the device to force it to check in with the G Data ManagementServer.

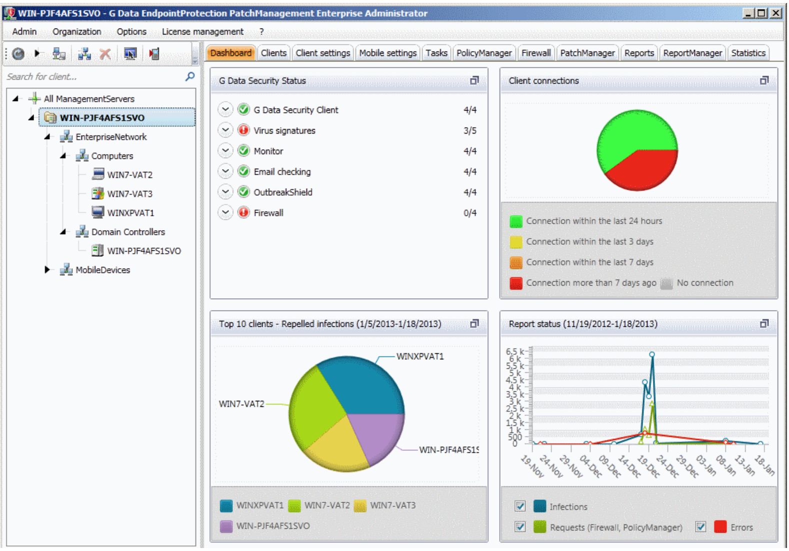
G Data ManagementServer

G Data 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. G Data ManagementServer uses the TCP/IP protocol to communicate with the clients. For clients that are temporarily disconnected from G Data ManagementServer, jobs are automatically accumulated and synchronized when communication is re-established. G Data ManagementServer has a central Quarantine folder. Suspicious files can be encrypted and secured, deleted, disinfected or forwarded to the G Data Security Labs if necessary. G Data ManagementServer is managed using **G Data Administrator**.

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

G Data Administrator

G Data Administrator is the administration software for G Data ManagementServer. It enables management of settings and updates for all G Data clients in the network. G Data Administrator is password-protected and can be installed to and launched from any Windows computer in the network. Scan jobs, backup jobs, security monitoring, and many more settings can be managed through Administrator. Automatic client installations and software and virus signature updates are also defined using Administrator.



WIN-PJF4AFS1SVO - G Data EndpointProtection PatchManagement Enterprise Administrator

G Data Security Status

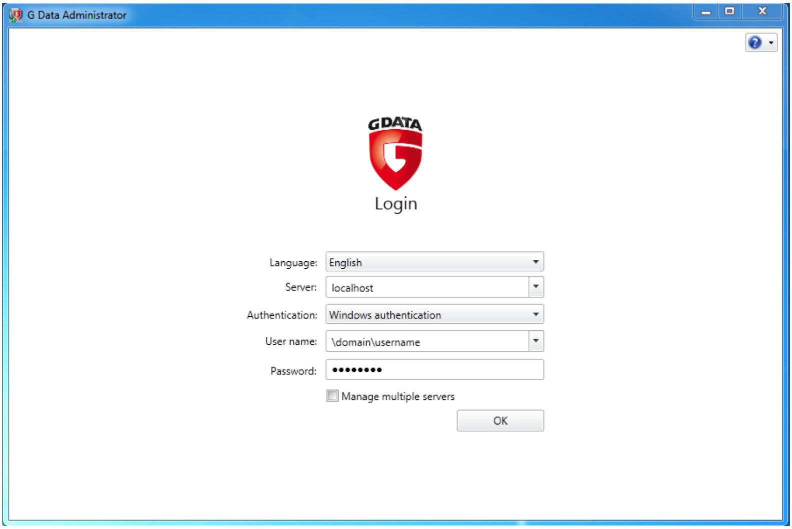
G Data Security Client	4/4
Virus signatures	3/5
Monitor	4/4
Email checking	4/4
OutbreakShield	4/4
Firewall	0/4

The Administrator interface is organized as follows: the **client management area** found on the left displays all clients which have been enabled, and to which G Data Client software can be or has already been deployed. To the right, all **modules** are accessible via dedicated tabs. The content of the module usually relates to the client or group of clients highlighted in the client management area. Above the client management and modules areas there is a menu bar for global settings and client organization, with additional menus that are only displayed when specific modules are selected.

When administering Linux clients which are installed on Samba servers, some options are blocked. For example, functions which are involved in handling emails are not available 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.

Starting G Data Administrator

The administration tool for managing G Data ManagementServer is accessed by clicking on the **G Data Administrator** option in the program group **Start** > **(All) Programs** > **G Data** > **G Data Administrator**.



Language: English

Server: localhost

Authentication: Windows authentication

User name: \domain\username

Password: ••••••••

□ Manage multiple servers

When starting G Data Administrator, you will be prompted for the **server**, **authentication type**, **user name** and **password**. In the Server field, enter the name of the computer on which G Data ManagementServer was installed, then select your **authentication** type:

- **Windows authentication**: If you have installed a SQL Server Express database for G Data ManagementServer, select the Windows authentication option and log in using your Windows administrator credentials.

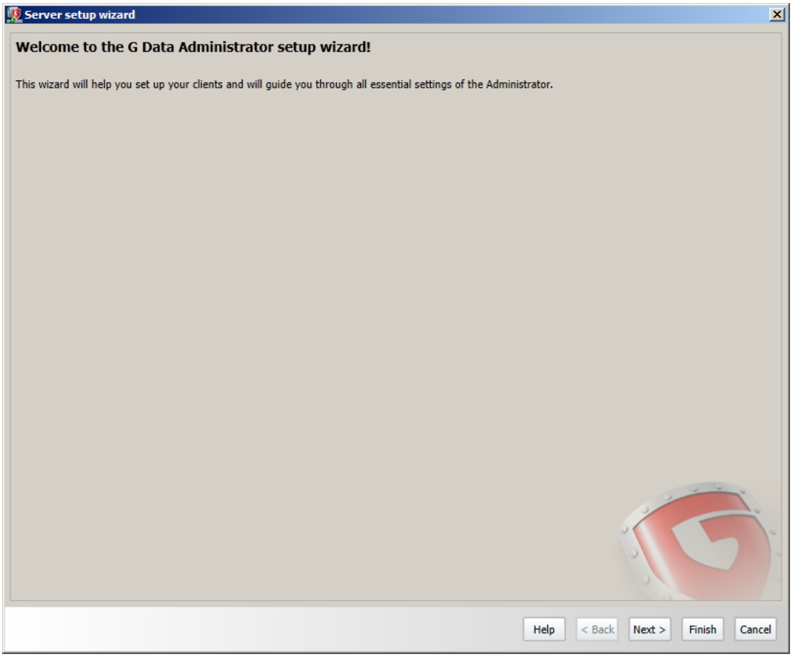
- **SQL integrated authentication**: If you are using an existing SQL Server instance, select the SQL integrated authentication option and log in using your SQL Server credentials.
- **Integrated authentication**: Log in using G Data ManagementServer's integrated authentication system. Integrated authentication accounts can be set up using the function **User account management**.

Configuring G Data Administrator

Administrative tasks

Server setup wizard

The Server setup wizard enables you to select and enable clients in the network on which the G Data software should be installed. It is automatically run the first time you start G Data Administrator, but can also be started afterwards through the **Admin** menu.



Server setup wizard

Welcome to the G Data Administrator setup wizard!

This wizard will help you set up your clients and will guide you through all essential settings of the Administrator.

Enable

All clients that are to be monitored by the G Data software must first be "enabled". To do this, highlight the clients to be enabled and click the **Enable** button. 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 and Printer Sharing). To enable these clients, enter the name of the computer in the **Computer** input field. After clicking on **Enable,** the computer 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 unticking it.

Internet update

G Data ManagementServer can download new virus signatures and program files over the Internet. For regular automatic updates, entering the **access data** created during the online registration is required. A detailed description for the scheduling of update intervals can be found in the section **Internet update**. You can also use the Internet update window to automate Internet updates afterwards.

Email notification

In the event of a virus discovery or other critical situations on one or more clients, the network administrator can be informed via email. Select the **recipient group(s)** or click the cogs icon to open the **Email settings**. 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

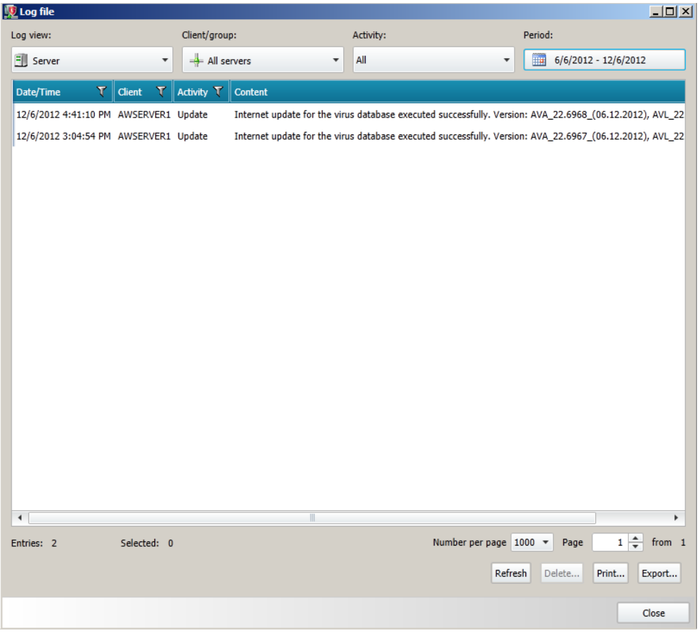
If you checked the option **Automatically install client software on the enabled computers**, the Server setup wizard will conclude by initiating the **remote installation** of G Data Security Client for all selected machines.

Display log

In the log file you will find an overview of the latest completed G Data software actions. The log display can be filtered according to the following criteria:

- **Log view**: Specify whether you would like to see a log of client or server procedures.
- **Client/group**: Specify whether you would like to view a log for all clients, groups, or an individual client.
- **Activity**: Define whether you would like to view all logged information or only notifications on specific topics.
- **Time**: Specify the from/to time range for which log information should be displayed.

Logs are displayed in chronological order and can be sorted according to specific criteria by clicking on the respective column header.



Log view: Server

Client/group: All servers

Activity: All

Period: 6/6/2012 - 12/6/2012

Date/Time	Client	Activity	Content
12/6/2012 4:41:10 PM	AWSERVER1	Update	Internet update for the virus database executed successfully. Version: AVA_22.6968_(06.12.2012), AVL_22
12/6/2012 3:04:54 PM	AWSERVER1	Update	Internet update for the virus database executed successfully. Version: AVA_22.6967_(06.12.2012), AVL_22

Entries: 2

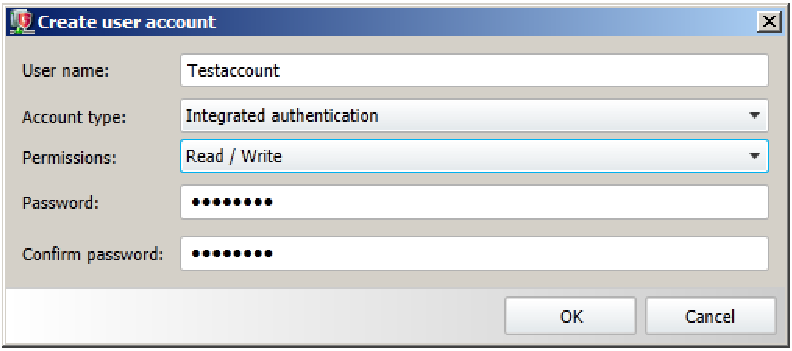
Selected: 0

Number per page 1000

Page 1 from 1

User account management

As system administrator, you can authorize additional users to have access to G Data Administrator. Click on the **New** button, then enter the user name, the **permissions** for this user (**Read only**, **Read/Write**, **Read/Write/Restore backups**), define the **account type** (**integrated authentication**, **Windows user**, **Windows user group**) and enter a **password** for this user.

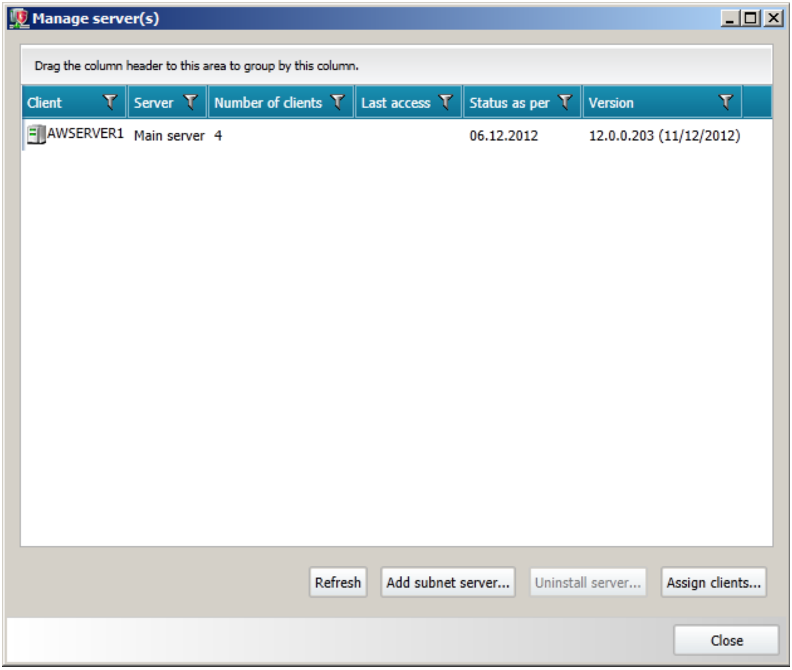


User name: Testaccount
Account type: Integrated authentication
Permissions: Read / Write
Password: ●●●●●●●●●
Confirm password: ●●●●●●●●●

Manage server(s)

Using the Manage Server function, you can assign clients or groups to individual subnet servers, which then bundle the communication of these clients with the main server to optimize network utilization. You can add subnet servers using this menu. By clicking the **Assign Clients** button, you can assign existing clients or groups to the defined subnet servers.

> The allocation of clients or groups to subnet servers functions separately from the grouping of clients. That means that clients that are assigned to different subnet servers can still be grouped together.



Client	Server	Number of clients	Last access	Status as per	Version
AWSERVER1	Main server	4		06.12.2012	12.0.0.203 (11/12/2012)

Synchronize subnet server(s)

To carry out changes outside the regular communication between server and subnet server, subnet server synchronization can be initiated manually.

Exit

This function closes G Data Administrator. G Data ManagementServer remains operational and manages network virus protection in accordance with the settings.

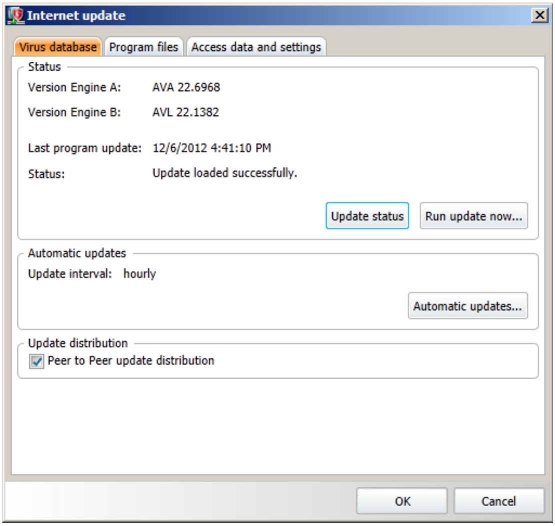
Options

Internet update

The Internet update window lets you specify settings for Internet updates for the virus databases and G Data software program files. On the tab **Access data and settings**, enter the access data that were created during the online registration. During the Internet update, the current virus definitions are downloaded from the G Data UpdateServer and saved on the G Data ManagementServer. Distribution of the virus signatures to the clients is managed through the **Clients** module. 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 no connection to the G Data ManagementServer or the Internet is available. Updating the virus signatures on clients takes place in two steps, which can both be automated. In the first step, the latest files from the G Data UpdateServer are downloaded to the G Data ManagementServer. In the second step, the new files are distributed to the clients (see **Client settings**).



Version Engine A: AVA 22.6968

Version Engine B: AVL 22.1382

Last program update: 12/6/2012 4:41:10 PM

Status: Update loaded successfully.

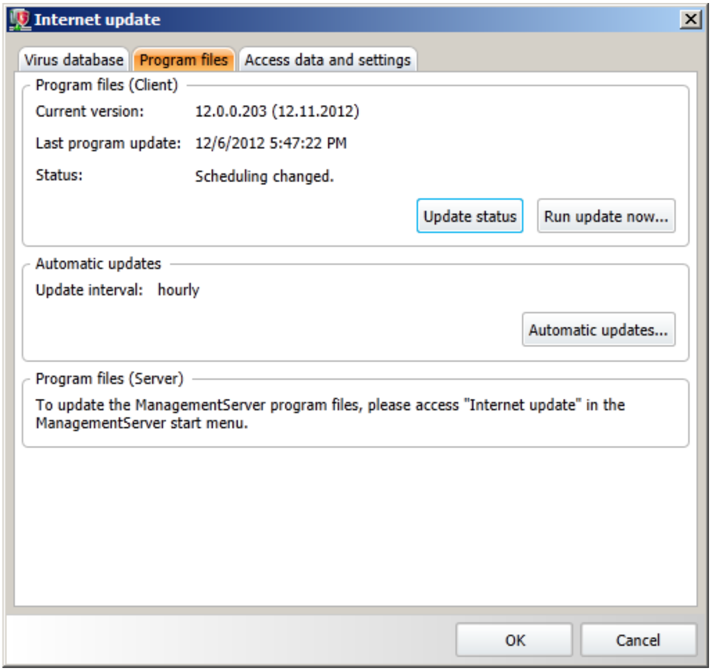
Update interval: hourly

☑ Peer to Peer update distribution

- **Update status**: Check the status of virus signatures, to take into account the latest changes.
- **Run update now**: Carry out an immediate update of the virus database. The current virus signatures are downloaded to be distributed to the clients afterwards.
- **Automatic updates**: As with virus checks, you can also let the Internet updates run automatically. To do this, check the box 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 ManagementServer must be connected to the Internet and you must have entered the user name and password that you have received upon registration. If the server connects to the Internet via a proxy server, your proxy credentials must be entered under **Access data and settings** > **Proxy settings**.
- **Update distribution**: Updates can be distributed centrally (MMS, subnet server > Clients) or, if you activate **Peer to Peer update distribution**, decentralised (MMS, subnet server, already updated client > Clients). Be sure to check the **port requirements** for this option.

Program files (Client)

When there is a client program file update, you can allow the clients to be updated automatically by G Data ManagementServer. Updating the program files on clients takes place in two steps, which can both be automated. In the first step, G Data ManagementServer downloads the latest files from the G Data UpdateServer. In the second step, the new files are distributed to the clients (see **Client settings**).



Program files (Client)

Current version: 12.0.0.203 (12.11.2012)

Last program update: 12/6/2012 5:47:22 PM

Status: Scheduling changed.

Automatic updates

Update interval: hourly

Program files (Server)

To update the ManagementServer program files, please access "Internet update" in the ManagementServer start menu.

- **Update status**: Check the status of program files, to take into account the latest changes.
- **Run update now**: Carry out an immediate update of the program files. The current program files are downloaded to be distributed to the clients afterwards.

- **Automatic updates**: As with virus checks, you can also let the Internet updates run automatically. To do this, check the box 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 ManagementServer must be connected to the Internet and you must have entered the user name and password that you have received upon registration. If the server connects to the Internet via a proxy server, your proxy credentials must be entered under **Access data and settings** > **Proxy settings**.

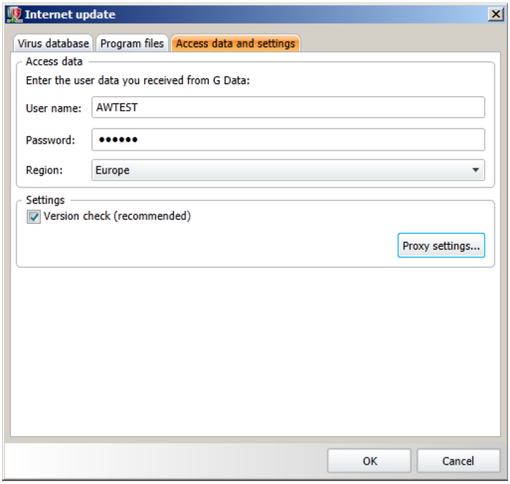
> To update the G Data ManagementServer program files, select the **G Data ManagementServer** program group, then select the **Internet update** entry from the start menu. G Data ManagementServer can only be updated via the Start menu, as opposed to the G Data Client software which can also be updated via G Data Administrator.

Access data and settings

With your online registration you received an email from G Data which includes your access data for updating the virus databases and program files. Enter these under **User name** and **Password**. The **version check** (enabled by default) should always be switched on because it prevents the downloading of unnecessarily large updates. If, however, problems arise with virus databases, switch off the version check. The current full version of the virus database will then be automatically downloaded to your server during the next Internet update.

Proxy settings opens a window in which proxy server credentials can be entered. You should only enter these if an Internet update cannot be executed without a proxy server.

> G Data software can use the Internet Explorer proxy 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*. In the **Proxy settings** window, switch off the option **Use proxy server**. Under **User account,** enter the account for which you have configured Internet Explorer (the account with which you have logged in to your computer).



Access data

Enter the user data you received from G Data:

User name: AWTEST

Password: ••••••

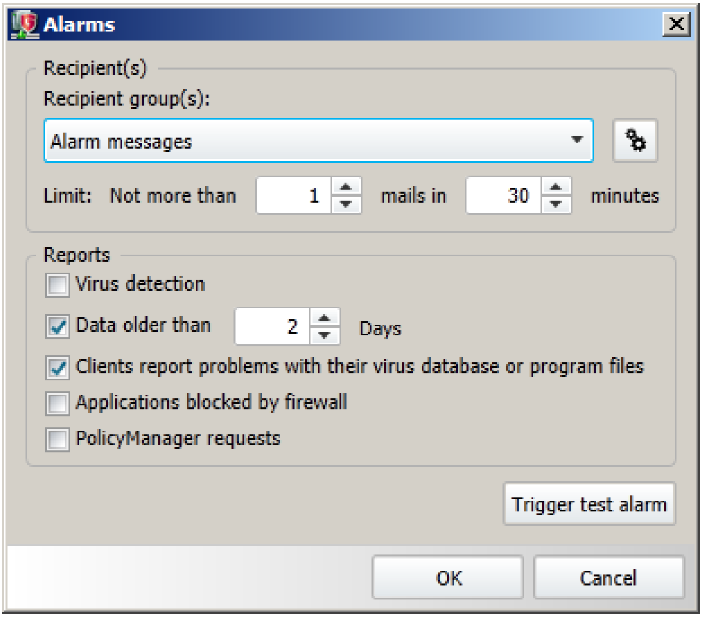
Region: Europe

Settings

☑ Version check (recommended)

Alarms

If a new virus is found, G Data ManagementServer can automatically send alarm notifications via email. Enable email notification by selecting the appropriate reports (**Virus detection**, **PolicyManager requests**, etc.). Select the intended recipient under **Recipient group(s)**. You can use the **limit** to prevent an excessive amount of email traffic in the event of a massive virus attack.



Alarms

Recipient(s)

Recipient group(s): Alarm messages

Limit: Not more than 1 mails in 30 minutes

Reports

□ Virus detection

☑ Data older than 2 Days

☑ Clients report problems with their virus database or program files

□ Applications blocked by firewall

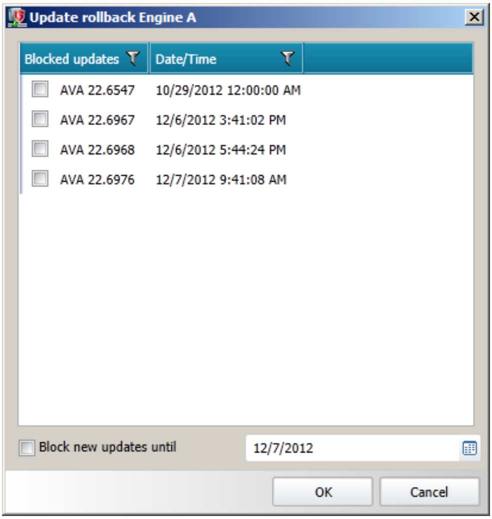
□ PolicyManager requests

Click the cogs icon (⚙) to open the **email settings** window and define recipient groups.

Update rollback Engine A/B

If, in rare cases, a false alarm or similar problems occur, it can make sense to block the latest update of the virus signatures and use a previous virus signature update instead. G Data 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 distribute a prior signature update to the clients and subnet servers. The number of rollbacks to be saved can be specified in the **Server settings**. The last five signature states are saved by default.

> On clients that are not connected to G Data 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 G Data ManagementServer.

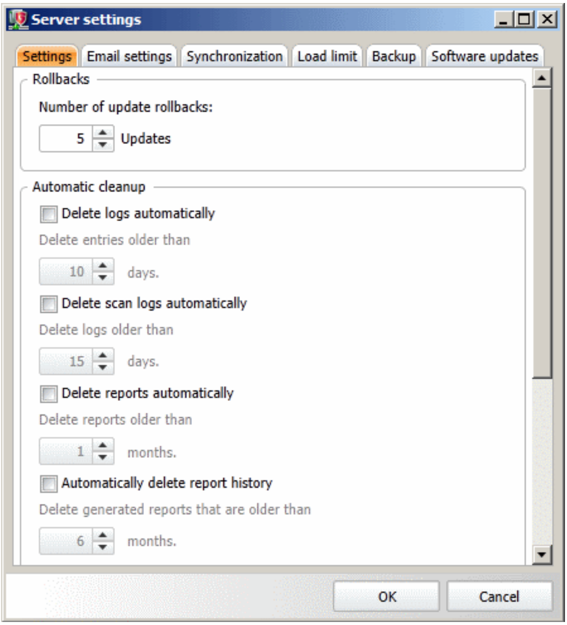


	Blocked updates	Date/Time
□	AVA 22.6547	10/29/2012 12:00:00 AM
□	AVA 22.6967	12/6/2012 3:41:02 PM
□	AVA 22.6968	12/6/2012 5:44:24 PM
□	AVA 22.6976	12/7/2012 9:41:08 AM

□ Block new updates until 12/7/2012

Server settings

Settings



Rollbacks

Number of update rollbacks:

5 Updates

Automatic cleanup

□ Delete logs automatically

Delete entries older than

10 days.

□ Delete scan logs automatically

Delete logs older than

15 days.

□ Delete reports automatically

Delete reports older than

1 months.

□ Automatically delete report history

Delete generated reports that are older than

6 months.

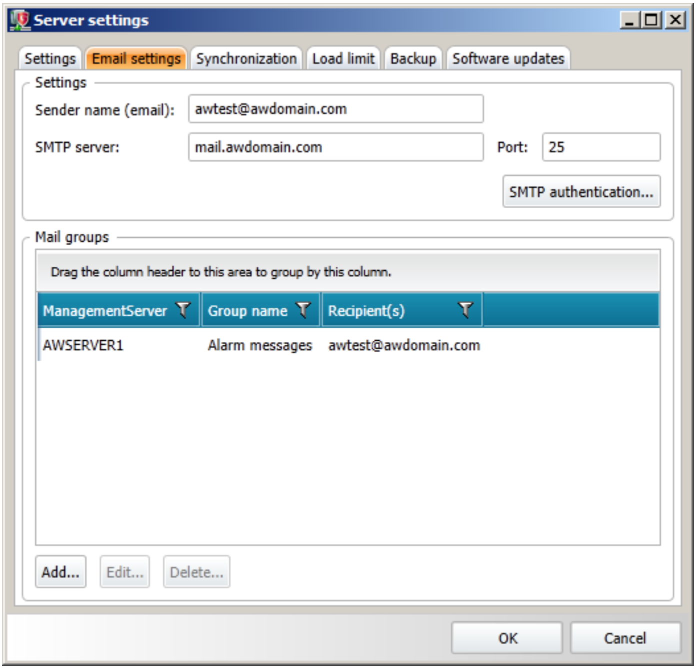
- **Rollbacks**: Indicate how many of the updated virus signature updates you would like to hold as a reserve for **engine rollbacks**. The default value here is the last five signature updates for each engine.
- **Automatic cleanup**: Configure whether various items should automatically be deleted after a specified period of time.
  - **Delete logs automatically**: Delete log files that are older than the set amount of days.
  - **Delete scan logs automatically**: Delete scan log files that are older than the set amount of days.
  - **Delete reports automatically**: Delete reports that are older than the set amount of months.
  - **Automatically delete report history**: Delete generated ReportManager reports that are older than the set amount of months.

  - ○ **Automatically delete clients following inactivity**: Delete clients that have not logged on for a set amount of days.
  - ○ **Automatically delete patch files**: Delete patch files that have not been used for more than the set amount of days.
- **Authentication for mobile clients**: Define the password with which mobile clients authenticate with G Data ManagementServer.

Email settings

Enter the **SMTP server** and **port** (normally 25) that G Data ManagementServer should use to send email. 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.

Under **Mail groups** you can manage recipient lists, such as Management or Administrators.



Settings

Sender name (email): awtest@awdomain.com

SMTP server: mail.awdomain.com Port: 25

Mail groups

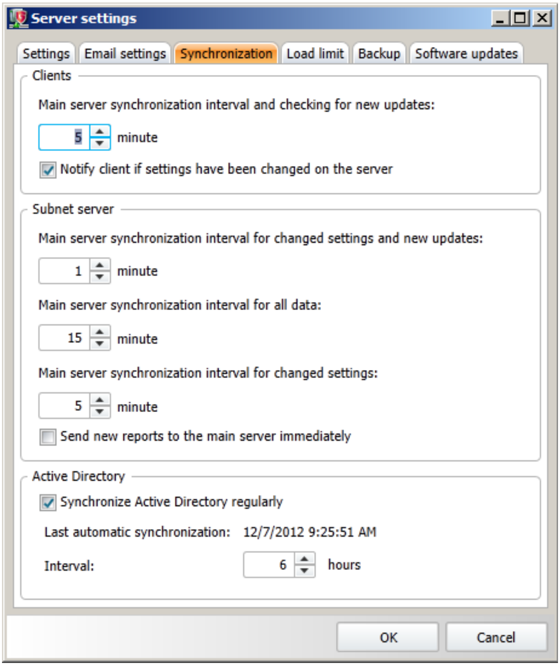
Drag the column header to this area to group by this column.

ManagementServer	Group name	Recipient(s)
AWSERVER1	Alarm messages	awtest@awdomain.com

Synchronization

In the Synchronization area, you can define the synchronization interval between clients, subnet servers and servers:

- **Clients**: Enter the time interval in which the clients are synchronized with the server. The default value is five minutes. If you tick **Notify client if settings have been changed on the server**, client PCs are immediately notified of new settings, regardless of synchronization interval.
- **Subnet server**: Define the intervals for communication between server and subnet server. If you tick **Send new reports to the main server immediately**, the reports will be transferred to the main server immediately, independently of the settings made here.
- **Active Directory:** define the interval with which G Data ManagementServer should synchronize Active Directory content. Active Directory synchronization only takes place if at least one group has been **assigned** an Active Directory Organizational Unit.



Clients

Main server synchronization interval and checking for new updates:

5 minute

☑ Notify client if settings have been changed on the server

Subnet server

Main server synchronization interval for changed settings and new updates:

1 minute

Main server synchronization interval for all data:

15 minute

Main server synchronization interval for changed settings:

5 minute

☐ Send new reports to the main server immediately

Active Directory

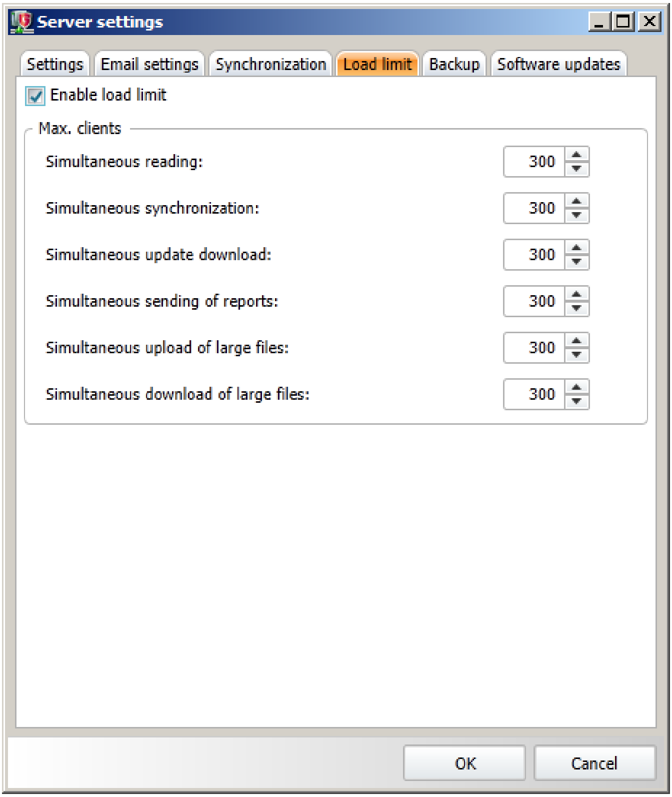
☑ Synchronize Active Directory regularly

Last automatic synchronization: 12/7/2012 9:25:51 AM

Interval: 6 hours

Load limit

If the checkbox next to **Enable load limit** is ticked, you can specify how many clients can simultaneously perform the actions listed. The load can be distributed so that simultaneous updates or reports do not cause an increase in network latency.



☑ Enable load limit

Max. clients

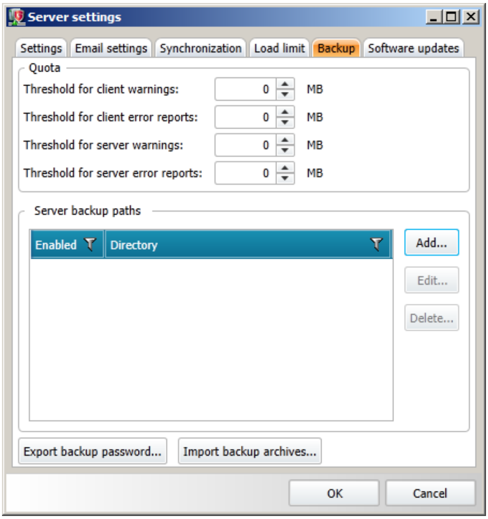
Simultaneous reading:	300
Simultaneous synchronization:	300
Simultaneous update download:	300
Simultaneous sending of reports:	300
Simultaneous upload of large files:	300
Simultaneous download of large files:	300

Backup

Thresholds for the amount of free storage space can be set in the **Quota** area. This is especially useful if a certain amount of disk space must always be available 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** when 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 where 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**.

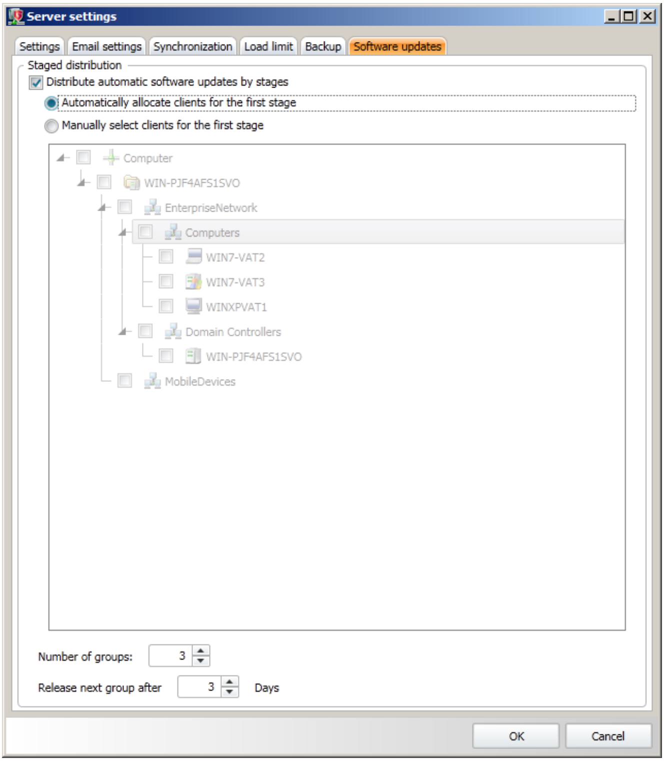
As all backups generated by the G Data software are encrypted, there is also the option of exporting backup passwords and saving them for later use. The **Import backup archives** button enables access to backups that are stored in other folders.



Threshold for client warnings: 0 MB
Threshold for client error reports: 0 MB
Threshold for server warnings: 0 MB
Threshold for server error reports: 0 MB

Software updates

Under **Staged distribution** you can set the distribution of software updates to be staged or to happen immediately. Staged distribution ensures that software updates do not cause problems in the network environment and decreases the system load of simultaneous program updates. When you enable staged distribution, you can choose to have the clients for the first group be defined automatically, or manually pick the clients that should be the first to receive software updates. You can also choose the total **number of groups** and the delay between distribution among the different groups.



☑ Distribute automatic software updates by stages

● Automatically allocate clients for the first stage

○ Manually select clients for the first stage

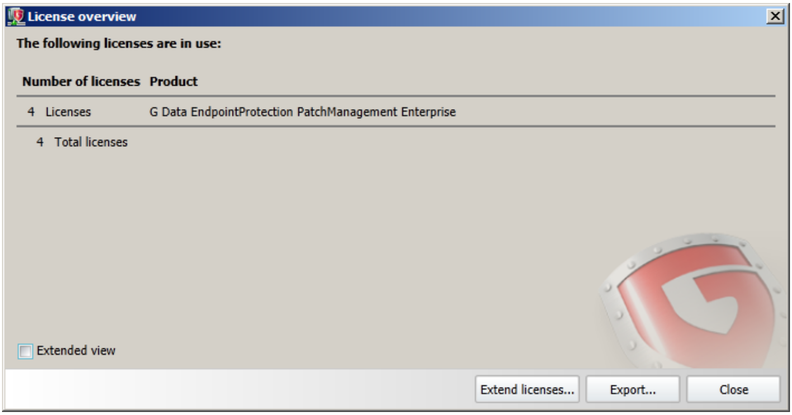
Number of groups: 3

Release next group after 3 Days

License management

Using License management you can have an overview of the amount of G Data software licenses that have been installed in your network. If you need additional licenses, you can get in contact with the G Data UpgradeCenter at any time by clicking **Extend licenses**.

Using the button **Export** you can export the overview to a text file. By selecting **Extended view**, you get specific information about the servers on which the licenses are being used.



The following licenses are in use:

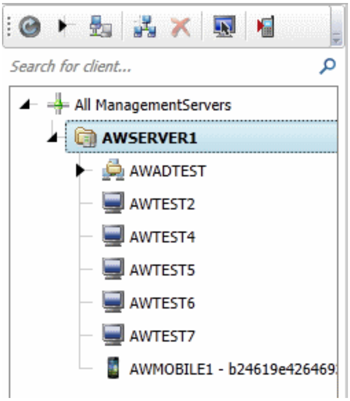
Number of licenses	Product
4 Licenses	G Data EndpointProtection PatchManagement Enterprise
4 Total licenses	

Help

Here, you can access software version information and also have the option of accessing the online help function.

Managing clients

All clients, servers, and groups in your network are listed in the client management area. As in Windows Explorer, groups that have subdivisions appear with a small plus symbol. If you click on them, the directory structure expands and enables the view of the structure below it. Clicking the minus symbol collapses the list. Depending on the type of client you select, different modules and options are available. For example, for PCs, the tab **Client settings** will be enabled which allows you to manage their options. For mobile clients, on the other hand, you get access to the **Mobile settings** tab.



Active Directory support

The Active Directory support of G Data Administrator imports all computer objects for the domain's organization units. For this, a separate group must be set up. When you right-click on the newly created group, the **Assign AD item to group** option appears. In the dialogue window that opens, select the **Assign to AD group** item and select the LDAP server. The **Select...** button provides a list of available servers. It is also possible to connect to another domain by clicking **Add**. The option **Automatically install G Data Security Client on newly added computers** has the effect that the client will immediately be installed on every computer that is added to the Active Directory domain, as long as it meets the **remote installation requirements**.

G Data ManagementServer compares its data status with the Active Directory every 60 minutes. This value can be changed under **Server settings** > **Synchronization**.

Icons and toolbar

The following icons are visible in the client management area:

Network

Group

Server (enabled)

Server (disabled)

Client (enabled)

Client (disabled)

Linux client (enabled)

Linux client (disabled)

Linux server (enabled)

Linux server (disabled)

Laptop client (enabled)

Laptop client (disabled)

Mobile client (enabled)

Mobile client (disabled)

Non-selectable devices: Devices like network printers fall under this category

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

Refresh: Use Refresh or the **F5** key to update the display of the Administrator interface at any time to take into account the latest changes

Expand/reduce all: With this button you can expand or collapse items in the network tree.

Show disabled clients: Select this button to display disabled computers. You can recognize the disabled computers by their greyed-out icons. Computers without file sharing or printer sharing are normally not shown at all.

Create new group: Enabled computers can be grouped. 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 (sub)group, select a server or group, and then click the toolbar button.

Delete: You can remove a computer from the list by highlighting it and then clicking 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 click the Enable button.

Send installation link to mobile clients: To manage mobile clients from within G Data Administrator, send them an installation link to the G Data MobileSecurity app. This initiates the **installation procedure for G Data MobileSecurity**.

Organization

Clients can be managed in the **client management tree structure** on the left side of the interface. Additional options are available through the Organization menu.

Refresh

You can use the **Refresh** function to update the client list in the client management area.

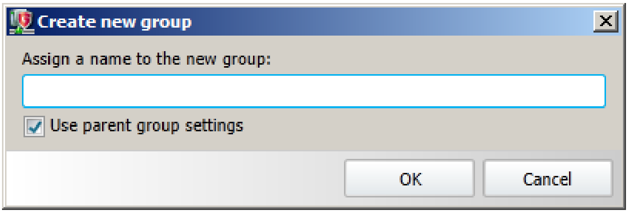
Show disabled clients

Clients that you have not (yet) enabled can be shown using this function. Disabled clients are then shown as greyed out icons.

In contrast, enabled clients are displayed as full-color icons.

Create new group

Clients can be combined into groups to apply settings to multiple clients at once. After selecting this option and entering a group name, clients can be assigned to the new group by dragging and dropping the desired client onto it.



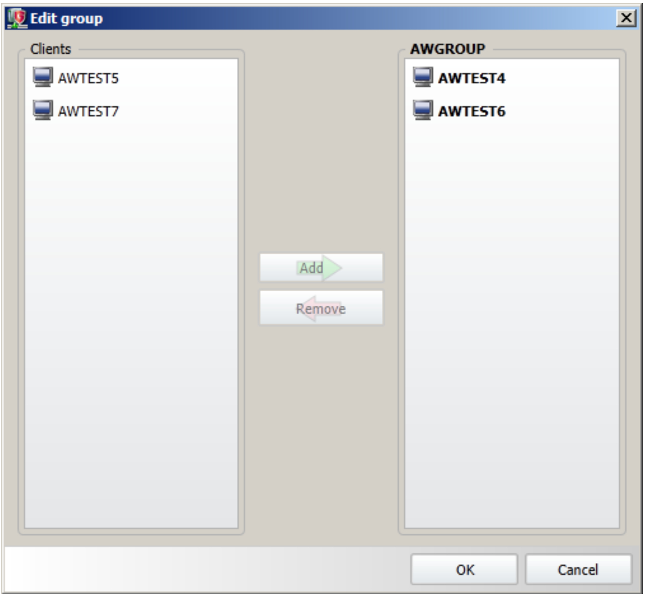
Create new group

Assign a name to the new group:

☑ Use parent group settings

Edit group

The **Edit group** option opens a window where the **Add** and **Remove** buttons can be used to add clients to groups or remove them from groups. This option is only available when a group is selected in the client management 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 other groups as necessary. Only empty groups can be deleted.

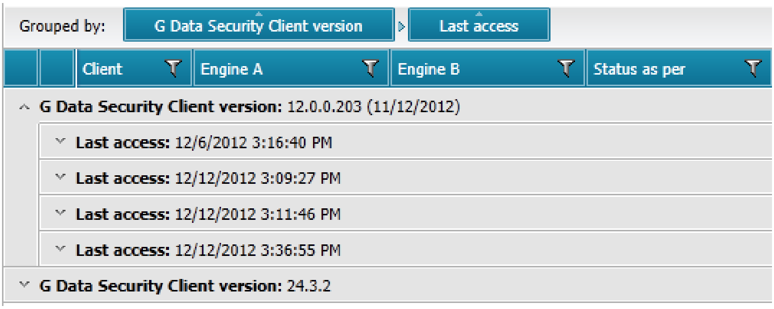
Create G Data Security Client install package

This function can be used to create an installation package for G Data Security Client. Use the package to install G Data Security Client locally without user interaction. See the chapter **Local installation** for more details.

Modules

Security settings and enterprise policies for the complete network and its clients can be configured using the various modules that you can select via the respective tabs. Each module's settings always apply to the clients or groups highlighted in the **Client management area**. The various modules are explained in detail in the following sections.

For most modules, there are general options to control layout and list contents. For example, to reduce the amount of items per page, enter the maximum **Number per page** at the bottom right of the screen. For free form text filtering, click any of the filter icons in the column headers and enter your filter criteria. An alternative to filtering list items is the use of groups. Drag one or more column headers to the bar above the column headers to create a group based on those columns. Groups can be nested in various ways to create different views.



Grouped by: G Data Security Client version ▸ Last access

		Client	Engine A	Engine B	Status as per

G Data Security Client version: 12.0.0.203 (11/12/2012)

Last access: 12/6/2012 3:16:40 PM

Last access: 12/12/2012 3:09:27 PM

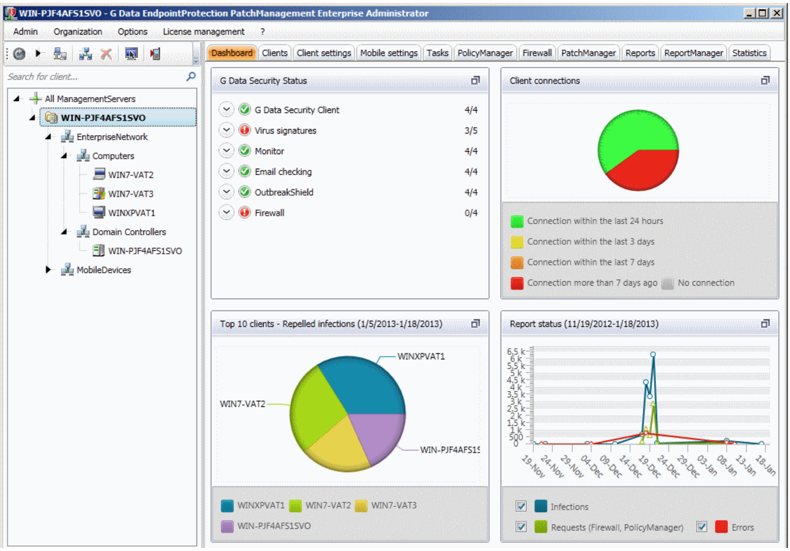
Last access: 12/12/2012 3:11:46 PM

Last access: 12/12/2012 3:36:55 PM

G Data Security Client version: 24.3.2

Dashboard

The Dashboard module shows information about the current status of the clients in the network.



G Data Security Status

✓ G Data Security Client	4/4
! Virus signatures	3/5
✓ Monitor	4/4
✓ Email checking	4/4
✓ OutbreakShield	4/4
! Firewall	0/4

G Data Security Status

Check all the basic security settings for the clients or groups that you have highlighted in the client management area and immediately deploy changes if necessary.

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

If a component is not optimally set (e.g. the monitor is switched off or a client's virus signatures are out of date), a warning symbol will alert you.

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

By clicking on the respective entry, you can directly carry out configuration changes or open the respective module. As soon as you have corrected the settings for a component with a warning icon, the warning icon will revert to the green icon.

Client connections

This gives you an overview chart of the connections that have been made to G Data ManagementServer. Using the chart you can make sure that all clients are regularly connecting to G Data ManagementServer.

Top 10 clients - Repelled infections

The clients that appear in this list should be monitored especially carefully. The appearance of one or more clients can indicate that the client users should be notified of possible problems, or that technical measures should be taken. If infections are taking place as a result of usage behavior, use of the **PolicyManager** module (available as part of the **G Data EndpointProtection** solution) might be advisable.

Report status

Report status offers visual representation of the number of infections, queries, and errors in your network during a configurable time period.

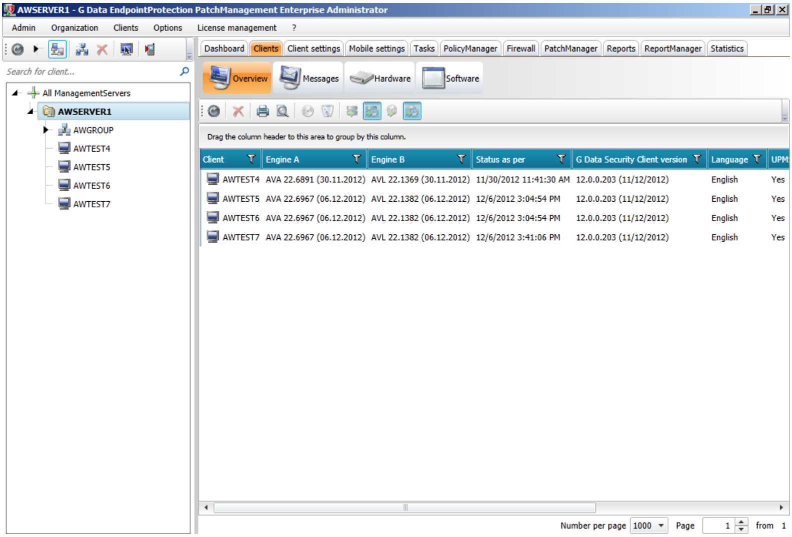
Clients

In the **client management area,** select a client or group. The version of the installed client, the version of the virus signatures and the last time the client reported to G Data ManagementServer will be displayed on the Clients tab for each client. This enables you to check whether the clients are running normally and if the virus signatures are fully up to date.

Using the buttons located at the top of the tab, you can decide whether you want to get a general **Overview** of the clients or whether you want to send individual clients **Messages**. By sending messages, you can quickly and conveniently inform users of the client about changes to its status. The Clients module also offers a simple inventory of client **hardware** and **software**.

Overview

From the Overview panel, you obtain an overview of all managed clients and can also simultaneously carry out any client administration. The list of clients 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.



Drag the column header to this area to group by this column.

Client	Engine A	Engine B	Status as per	G Data Security Client version	Language	UPM
AWTEST4	AVA 22.6891 (30.11.2012)	AVL 22.1369 (30.11.2012)	11/30/2012 11:41:30 AM	12.0.0.203 (11/12/2012)	English	Yes
AWTEST5	AVA 22.6967 (06.12.2012)	AVL 22.1382 (06.12.2012)	12/6/2012 3:04:54 PM	12.0.0.203 (11/12/2012)	English	Yes
AWTEST6	AVA 22.6967 (06.12.2012)	AVL 22.1382 (06.12.2012)	12/6/2012 3:04:54 PM	12.0.0.203 (11/12/2012)	English	Yes
AWTEST7	AVA 22.6967 (06.12.2012)	AVL 22.1382 (06.12.2012)	12/6/2012 3:41:06 PM	12.0.0.203 (11/12/2012)	English	Yes

By right clicking any of the column headers and selecting **Select columns**, you can choose from a large number of properties to be displayed in the client overview:

- **Server**
- **Alias (server)**
- **Client**
- **Engine A**
- **Engine B**
- **Status as per**
- **G Data Security Client version**
- **Language**
- **UPMS client**
- **Last access**
- **Virus signature update/time**

- **Program update/time**
- **Operating system**
- **Subnet server**
- **Domain**
- **Network card**
- **MAC address**
- **IPv4 address**
- **IPv6 address**
- **Subnet mask**
- **Default gateway**
- **DNS server**
- **DHCP server**
- **Primary WINS**
- **Secondary WINS**

To manage the clients, you can use the following options from the toolbar above the list:

Refresh: This function updates the view and loads the current client list G Data ManagementServer.

Delete: Remove a client from the Client view.

Print: Print the client list. In the selection screen that appears, you can specify which details you would like to print.

Page view: Preview the page(s) to be printed.

Install G Data Security Client

Uninstall G Data Security Client

Update virus signatures now: Updates the virus database on the client with current signatures from G Data ManagementServer.

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

Update program files now: Updates the program files on the client with the current files from G Data ManagementServer. A client reboot may be necessary after updating the program files.

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

Menu bar

When the Overview panel is selected, an additional menu entry named **Clients** becomes available in the menu bar. It reflects the options that are also available by right-clicking one or more clients. The following options are included:

- **Install G Data Security Client**
- **Install G Data Security Client for Linux**
- **Uninstall G Data Security Client**
- **Reset to default**: Reset the security settings for (groups of) clients.
- **Move G Data Security Client to group**: This function allows you to move the selected client to an existing group. By selecting this function, all existing groups are displayed in a new dialog window. To move a client to a group, select the group and click **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 for individual clients.
- **Update virus signatures now**
- **Update virus signatures automatically**
- **Update program files now**
- **Update program files automatically**

- **Reboot after program update**: Define what should happen after client program file updates. Select **Open message box on client** to inform a user that they should restart his/her client computer at a convenient time. **Create report** will create a report in the **Reports** module, or select **Force reboot** to automatically force a restart.

Install G Data Security Client

Select the option Install G Data Security Client to initiate a **remote installation** of G Data Security Client on all selected machines.

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

If the software cannot be installed using the remote installation, you can also perform a **local installation** using the G Data software DVD or a client install package.

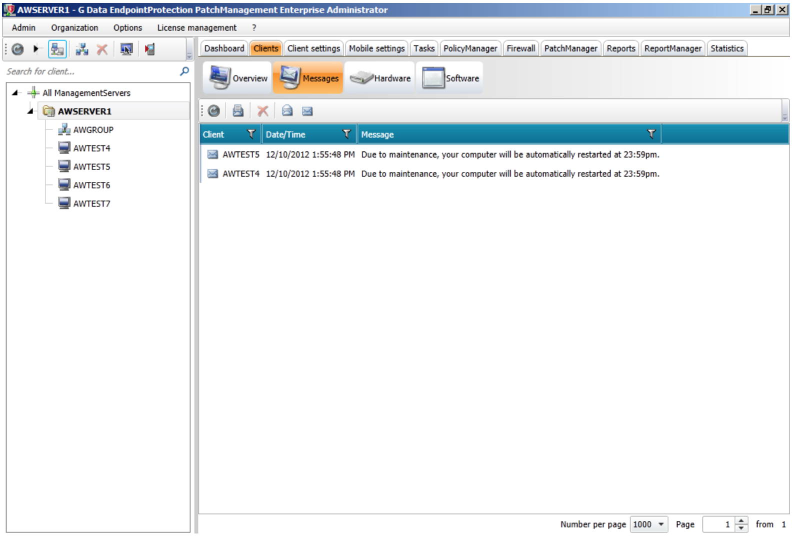
Uninstall G Data Security Client

Using this function prompts the G Data Security Client to uninstall itself. For a complete removal the client must be restarted. The user is prompted to do so.

Alternatively it is also possible to uninstall the client locally. This requires a command 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 it is not requested automatically, the computer must be restarted within 10 minutes.

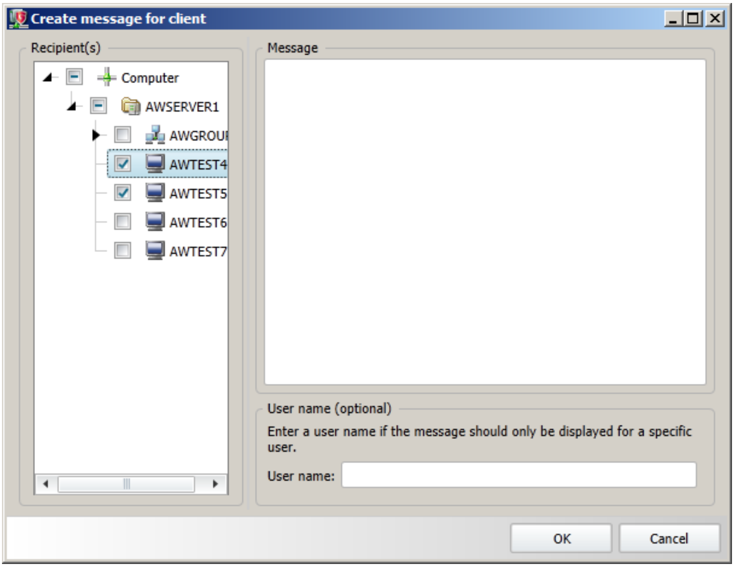
Messages

As a network administrator, you can send messages to individual clients or client groups to quickly and conveniently inform users about changes to their status. The messages are displayed as a small popup on the bottom right of the client desktop.



Client	Date/Time	Message
AWTEST5	12/10/2012 1:55:48 PM	Due to maintenance, your computer will be automatically restarted at 23:59pm.
AWTEST4	12/10/2012 1:55:48 PM	Due to maintenance, your computer will be automatically restarted at 23:59pm.

To create a message, simply click the **New** button. In the dialogue, you can select the clients you want to send the message to. If you want a message to be accessible only to certain users of a client computer or network, enter their login names under **User name**. Type your information in the **Message** field and click the **Send** button.

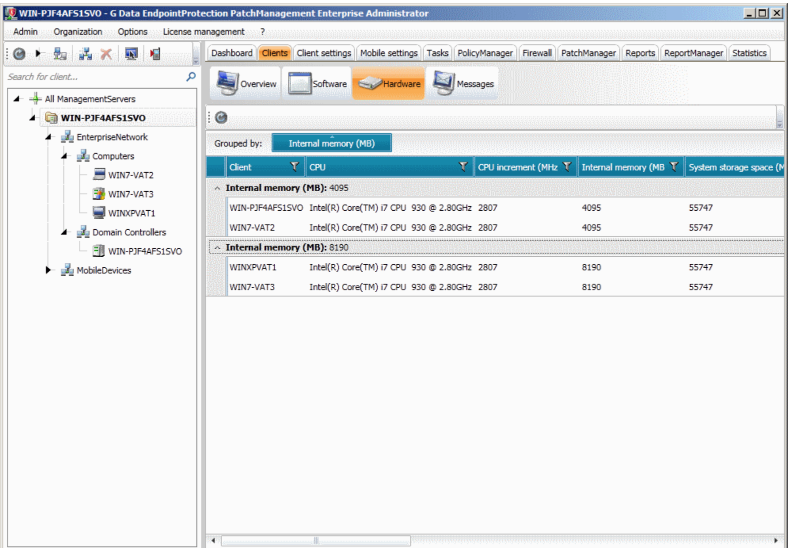


Enter a user name if the message should only be displayed for a specific user.

User name:

Hardware inventory

The Hardware inventory view shows you information about the hardware that is in use by clients.



Grouped by: Internal memory (MB)

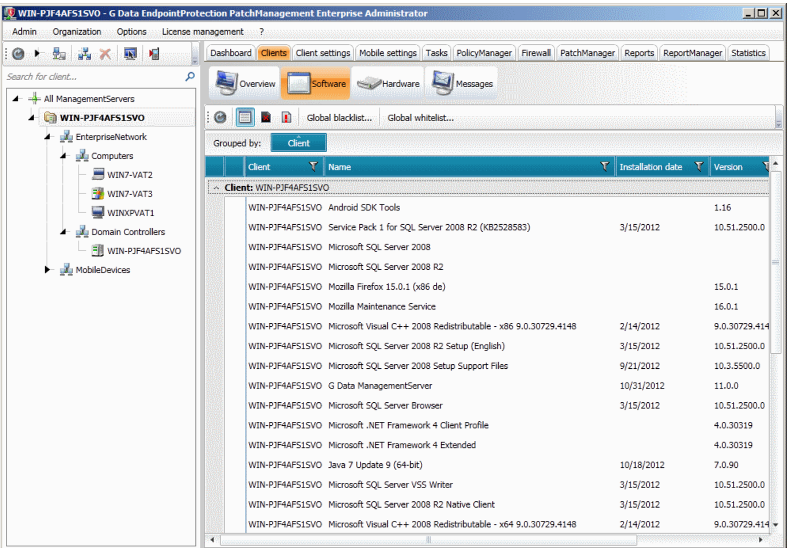
Client	CPU	CPU increment (MHz	Internal memory (MB	System storage space (M
Internal memory (MB): 4095				
WIN-PJF4AFS1SVO	Intel(R) Core(TM) i7 CPU 930 @ 2.80GHz	2807	4095	55747
WIN7-VAT2	Intel(R) Core(TM) i7 CPU 930 @ 2.80GHz	2807	4095	55747
Internal memory (MB): 8190				
WINXPVAT1	Intel(R) Core(TM) i7 CPU 930 @ 2.80GHz	2807	8190	55747
WIN7-VAT3	Intel(R) Core(TM) i7 CPU 930 @ 2.80GHz	2807	8190	55747

After a right click on the column headers, click **Select columns** to choose additional categories to display in the list view:

- **Client**
- **CPU**
- **CPU increment (MHz)**
- **Internal memory (MB)**
- **System storage space (MB)**
- **System storage space (statistics)**
- **Total storage space (MB)**
- **Total storage space (statistics)**
- **System manufacturer**
- **System name**
- **System version**
- **System family**
- **CPU ID**
- **Mainboard manufacturer**
- **Mainboard**
- **Mainboard version**
- **Bios manufacturer**
- **Bios publishing date**
- **Bios version**

Software inventory

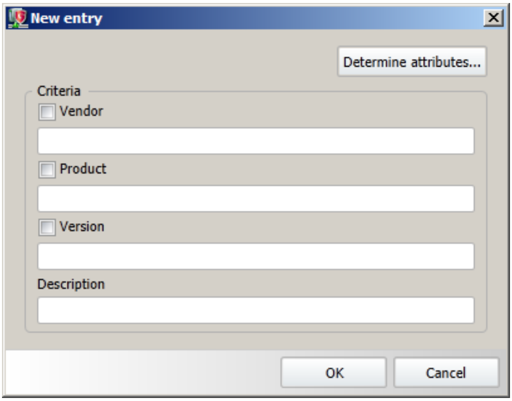
The software inventory allows you to monitor software use across the whole network. Software can be added to a blacklist or whitelist to serve as a base for decision making about network software management.



Client: WIN-PJF4AFS1SVO

Client	Name	Installation date	Version
WIN-PJF4AFS1SVO	Android SDK Tools		1.16
WIN-PJF4AFS1SVO	Service Pack 1 for SQL Server 2008 R2 (KB2528583)	3/15/2012	10.51.2500.0
WIN-PJF4AFS1SVO	Microsoft SQL Server 2008		
WIN-PJF4AFS1SVO	Microsoft SQL Server 2008 R2		
WIN-PJF4AFS1SVO	Mozilla Firefox 15.0.1 (x86 de)		15.0.1
WIN-PJF4AFS1SVO	Mozilla Maintenance Service		16.0.1
WIN-PJF4AFS1SVO	Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148	2/14/2012	9.0.30729.414
WIN-PJF4AFS1SVO	Microsoft SQL Server 2008 R2 Setup (English)	3/15/2012	10.51.2500.0
WIN-PJF4AFS1SVO	Microsoft SQL Server 2008 Setup Support Files	9/21/2012	10.3.5500.0
WIN-PJF4AFS1SVO	G Data ManagementServer	10/31/2012	11.0.0
WIN-PJF4AFS1SVO	Microsoft SQL Server Browser	3/15/2012	10.51.2500.0
WIN-PJF4AFS1SVO	Microsoft .NET Framework 4 Client Profile		4.0.30319
WIN-PJF4AFS1SVO	Microsoft .NET Framework 4 Extended		4.0.30319
WIN-PJF4AFS1SVO	Java 7 Update 9 (64-bit)	10/18/2012	7.0.90
WIN-PJF4AFS1SVO	Microsoft SQL Server VSS Writer	3/15/2012	10.51.2500.0
WIN-PJF4AFS1SVO	Microsoft SQL Server 2008 R2 Native Client	3/15/2012	10.51.2500.0
WIN-PJF4AFS1SVO	Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.4148	2/14/2012	9.0.30729.414

The list area lists installed software for all clients selected in the **client management area**. To fill the blacklist or whitelist, click the button **Global blacklist** or **Global whitelist**. Click **Add** to add a new blacklist or whitelist rule. The option **Determine attributes** lets you select the program you want to put on the blacklist or whitelist and enter its attributes. To set an attribute as rule, tick an attribute's checkbox. This allows you to put software from specific vendors, or specific program versions, on the lists. When you already know the program's attributes, you can also directly add them to the blacklist or whitelist, without using the Determine attributes dialog.



The list of items on the blacklist and whitelist can be managed with the following toolbar buttons:

Refresh: Refresh the blacklist and whitelist overview.

Display all: Display all software that has been installed on the clients.

Display only software on the blacklist: Only show software that you have blocked by adding it to the blacklist.

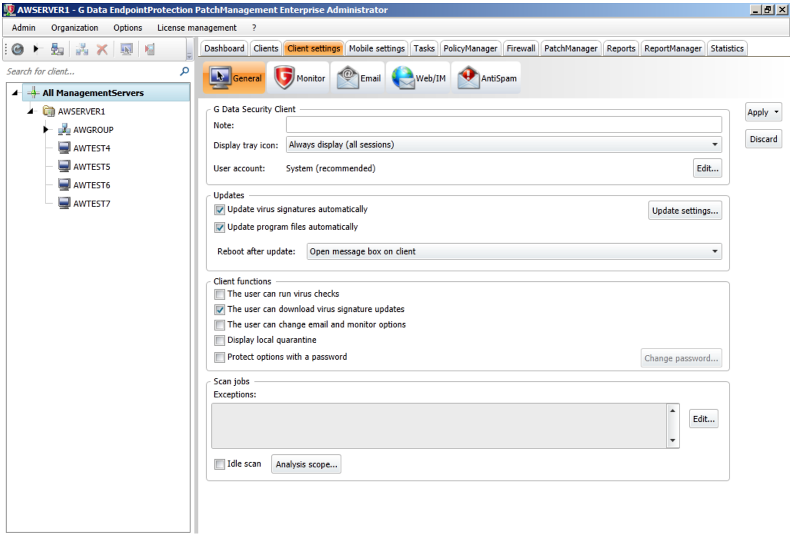
Display only software that is not on the whitelist: Only show software that is installed on the network clients, but has not been checked yet by the system administrator. Using this view, you can quickly add software to the blacklist or whitelist by right clicking on it.

Client settings

The Client settings module manages settings for individual clients or groups of clients. Using the General, Monitor, Email, Web/IM and AntiSpam options you can extensively configure protection for network clients.

General

The General tab allows you to set general settings for the selected clients.



G Data Security Client

Note:

Display tray icon: Always display (all sessions)

User account: System (recommended)

Updates

☑ Update virus signatures automatically

☑ Update program files automatically

Reboot after update: Open message box on client

Client functions

□ The user can run virus checks

☑ The user can download virus signature updates

□ The user can change email and monitor options

□ Display local quarantine

□ Protect options with a password

Scan jobs

Exceptions:

□ Idle scan

G Data Security Client

- **Note**: Enter any notes or remarks that apply to this client.
- **Display tray icon**: For terminal servers and Windows versions with fast user switching you can select the sessions in which a client icon should be displayed in the taskbar: **never**, **in first session only** (for terminal servers) or **always**. The icon must be displayed if you want to enable the user to have access to client options and functionality such as Idle Scan.
- **User account**: The client software normally runs on the system account. You can enter a different user account to provide the client with different permissions, for example to allow checking of network shares. This account needs to have administrator permissions on the client.

Updates

- **Update virus signatures automatically**: Enables automatic updating of the virus signatures. The clients periodically check whether new virus signatures exist on the G Data ManagementServer. If new virus signatures are available, they are automatically installed on the client.
- **Update program files automatically**: Enables automatic updating of the program files. The clients periodically check whether updated program files exist on the G Data ManagementServer. If updated program files are available, they are automatically installed on the client. A client reboot may be necessary after the update. Dependent on the setting under **Reboot after update,** the client user has the option of postponing the completion of the update.
- **Reboot after update**: Select **Open message box on client** to inform a user that they should restart their client computer at a convenient time. **Create report** will create a report in the **Reports** module, or select **Force reboot** to automatically force a restart.
- **Update settings**: Define where clients obtain their virus signature updates. There is the option of allowing clients to download virus signatures from the ManagementServer; alternatively you can grant them the right to obtain updates themselves. Mixed mode is recommended for mobile workstations. In that case, when the client has a connection to the ManagementServer, it gets the updates from there. If there is no connection to the ManagementServer, the virus signatures are automatically downloaded from the Internet. The **Settings and scheduling** button can be used to schedule virus signatures downloads at certain intervals.

Client functions

Under Client functions, you can set permissions for local users to use the Security Client. User rights can be very extensive or restrictive, as your network policy demands.

- **The user can run virus checks**: In case of a suspected virus infection, the user can run a local virus check, independent of the ManagementServer schedule. Results of this virus check will be transferred to the ManagementServer during the synchronization.

- **The user can download virus signature updates**: If you enable this function, the user of the client computer is allowed to download virus signatures over the Internet, without connecting to the ManagementServer. This is especially important if the client has a laptop that is often used outside the network perimeter.
- **The user can change email and monitor options**: If this function is enabled, the client user has the option to change the **Monitor**, **Email**, **Web/IM** and **AntiSpam** settings.
- **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. In doing so, note that a virus is not removed by restoring a file from quarantine. This option should therefore only be made accessible to experienced users.
- **Protect options with a password**: 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 from changing the settings. The password is set specifically for the selected client or group and it should only be shared with authorized users.

Scan jobs

You can define exceptions that are not to be checked during the execution of scan jobs. Archives and restore partitions, for example, can be defined as exception directories. You can also define file extensions as exceptions. Exceptions 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 preserved. The same procedure also goes for monitor exceptions.

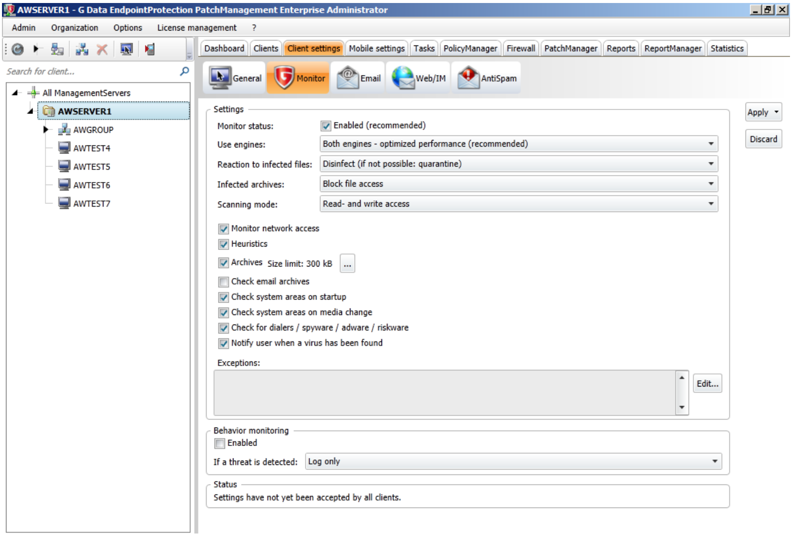
By clicking the **Analysis scope** button, you can define the scan scope, which includes all local hard drives by default. To allow the client to perform a virus scan when the computer is idle, tick **Idle scan**.

> Special note for Linux file servers: when selecting directory exceptions, the root drive (/) and all shares are listed. This way, drive, directory, and file exceptions can be created.

Monitor

The Monitor panel allows you to configure the most important aspects of client protection. The changed settings are only saved once the **Apply** button has been clicked. Click the **Discard** button to load the current settings from the ManagementServer without accepting the changes. If clients within a group have different settings for a specific option, the option will be allocated an undefined status. Undefined options are not saved during the transfer.

The monitor should not be disabled, as it provides real-time protection against malware. 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 troubleshooting. It is possible to define exceptions for the monitor. If an application suffers from performance loss due to use of the monitor, exceptions can be added for the relevant program files or processes; excluded files are then no longer checked by the monitor. Setting up monitoring exceptions can represent a security risk.



Settings

Monitor status: ☑ Enabled (recommended)

Use engines: Both engines - optimized performance (recommended)

Reaction to infected files: Disinfect (if not possible: quarantine)

Infected archives: Block file access

Scanning mode: Read- and write access

☑ Monitor network access

☑ Heuristics

☑ Archives Size limit: 300 kB ...

☐ Check email archives

☑ Check system areas on startup

☑ Check system areas on media change

☑ Check for dialers / spyware / adware / riskware

☑ Notify user when a virus has been found

Exceptions:

Behavior monitoring

☐ Enabled

If a threat is detected: Log only

Status

Settings have not yet been accepted by all clients.

Settings

- **Monitor status**: Switch the monitor on or off. In general you should leave the monitor switched on, as it is the foundation of permanent and uninterrupted virus protection.
- **Use engines**: The G Data software works with two independently operating virus scanning engines. Using both engines guarantees optimum results for preventing viruses. Using just one engine may have performance advantages.
- **Reaction to infected files**: Specify the action to be taken if an infected file is detected. There are various options that may or may not be suitable, depending on what the respective client is used for:
    - **Block file access**: Neither read nor write access will be granted for an infected file.
    - **Disinfect (if not possible: block file access)**: An attempt is made to remove the virus; if this is not possible, file access is blocked.
    - **Disinfect (if not possible: quarantine)**: An attempt is made to remove the virus; if this is not possible, the file is moved to Quarantine.
    - **Disinfect (if not possible: delete file)**: An attempt is made to remove the virus; if this is not possible, the file is deleted. 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. In the rare case of a false-positive virus message, this may lead to data loss.
- **Infected archives**: 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.

- **Scanning mode**: Define when files should be scanned. **Read access** scans every file directly when it's read. **Read- and write access** adds a scan on writing, to protect against viruses that are copied from another possibly unprotected client or from the Internet. **On execution** scans files only when they are executed.
- **Monitor network access**: Enable network access monitoring. If your entire network is already being monitored by G Data software, network access monitoring can be disabled.
- **Heuristics**: Through heuristic analysis, viruses are not only detected on the basis of the constantly updated virus databases, but also on characteristics typical of viruses. This method provides additional security, but may also produce a false alarm in rare cases.
- **Archives**: 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 that should be checked.
- **Check email archives**: This option should generally be disabled, as scanning email archives takes a long time, and if an infected email is found, the entire mailbox is moved to quarantine or deleted - depending on the virus scan settings. Email in the mail archive may no longer be available in such a case. As the monitor also blocks execution of email attachments, disabling this option does not create a security hole. Moreover, when using Outlook, incoming and outgoing mails are scanned using an integrated plug-in.
- **Check system areas on startup** / **media change**: System areas (boot sectors) in your computer should be included in virus checks. Here, you can specify whether these should be checked on system start-up and/or whenever a media change occurs (new DVD, etc.). Generally, you should have at least one of these two functions activated.

- **Check for dialers / spyware / adware / riskware**: You can use the G Data software to check your system for dialers and other malware programs (spyware, adware, riskware). This includes programs that establish unrequested expensive Internet connections and are potentially every bit as damaging as a virus in terms of economical impact. For example, spyware can silently record end user surfing behavior or keystrokes (including passwords) and forward this to third parties via the Internet.
- **Notify user when a virus has been found**: If this option is enabled, when a virus is found by the monitor, a notification window is displayed, informing the user that a virus has been found on the system. The file that has been found, its path and the name of the malware found are displayed.

Exceptions

You can exclude specific directories from virus check, for example to omit folders with archives that are seldom used in order to integrate them into a special scan job. Files and file types can also be excluded from the virus check. The following exceptions can be configured:

- **Drive**: Select a drive (partition, hard disk) that you do not want to be checked by the monitor.
- **Directory**: Select a folder (including any subfolder contained within it) that you do not want to be checked by the monitor.
- **File**: Enter the name of a file that you do not want to be checked by the monitor. You can also use wildcards.
- **Process**: If a specific process should not be monitored by the monitor, enter the name of the process concerned.

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

Wildcards work as follows: the question mark symbol (?) represents individual characters. The asterisk symbol (*) represents entire character strings. For instance, in order to exclude all files with the file extension **exe**, enter ***.exe**. To exclude files with different spreadsheet formats (e.g. **.xlr**, **.xls**), simply enter ***.xl?**. Or, to exclude 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.

Behavior monitoring

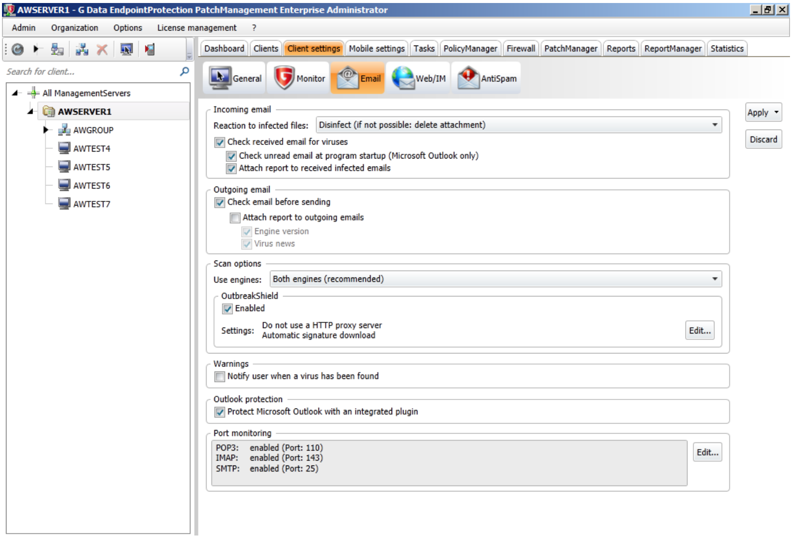
Behavior monitoring provides further protection against malicious files and processes. Unlike the monitor, it is not signature-based, but analyzes the actual behavior of a process. To undertake a classification, behavior monitoring uses various criteria, such as write access to the registry and the possible creation of auto-start entries. If sufficient criteria lead to the conclusion that a program is exhibiting suspicious behavior, the action set under **If a threat is detected** will be carried out. The options **Log only**, **Halt program,** and **Halt program and move to quarantine** are available here. With the setting **Log only,** the program is not impacted but a message is displayed under **Reports**.

Status

Here, you are shown whether the changes you have made to the monitor settings have already been applied to the client or group.

Email

Virus protection for email can be set up on every G Data Security Client. The default ports for the POP3, IMAP, and SMTP protocols will be monitored. Additionally, a special plugin for Microsoft Outlook automatically checks all incoming email for viruses and prevents infected email from being sent.



Incoming email
Reaction to infected files: Disinfect (if not possible: delete attachment)
☑ Check received email for viruses
☑ Check unread email at program startup (Microsoft Outlook only)
☑ Attach report to received infected emails

Outgoing email
☑ Check email before sending
☐ Attach report to outgoing emails
☑ Engine version
☑ Virus news

Scan options
Use engines: Both engines (recommended)
OutbreakShield
☑ Enabled
Settings: Do not use a HTTP proxy server
Automatic signature download

Warnings
☐ Notify user when a virus has been found

Outlook protection
☑ Protect Microsoft Outlook with an integrated plugin

Port monitoring
POP3: enabled (Port: 110)
IMAP: enabled (Port: 143)
SMTP: enabled (Port: 25)

Incoming email

- **In case of an infection**: 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 will be checked for viruses.
- **Check unread email at program start-up (Microsoft Outlook only)**: This option is used to scan emails for viruses that the client may receive while it is offline. All unread email in your Inbox folder and subfolders are checked as soon as you open Outlook.

- **Attach report to received infected emails**: 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 a *[VIRUS]* notification before the actual subject. If you enabled the option **Delete text/attachment**, you will also be notified that the infected part of the email was deleted.

Outgoing email

- **Check email before sending**: To make sure that you do not send out any infected emails, the G Data software offers the option of checking outgoing emails for viruses before sending them. If an email actually contains a virus, the message *The mail [subject header] contains the following virus: [virus name]* is added and the relevant email is not sent.
- **Attach report to outgoing emails**: A report is displayed in the body of each outgoing email below the actual mail text. It reads *Virus checked by G Data AntiVirus*, provided that you have enabled the **Check email before sending** option. G Data engine version info and virus news can also be added (**engine version**/**virus news**).

Scan options

- **Use engines**: The G Data software works with two independently operating virus scanning engines. Using both engines guarantees optimum results for preventing viruses. Using just one engine may have performance advantages.
- **OutbreakShield**: OutbreakShield detects and neutralizes 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, closing 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 allows OutbreakShield to carry out an automatic signature download from the Internet.

Warnings

- **Notify user when a virus has been found**: Recipients of an infected message will automatically be notified through a virus warning popup.

Outlook protection

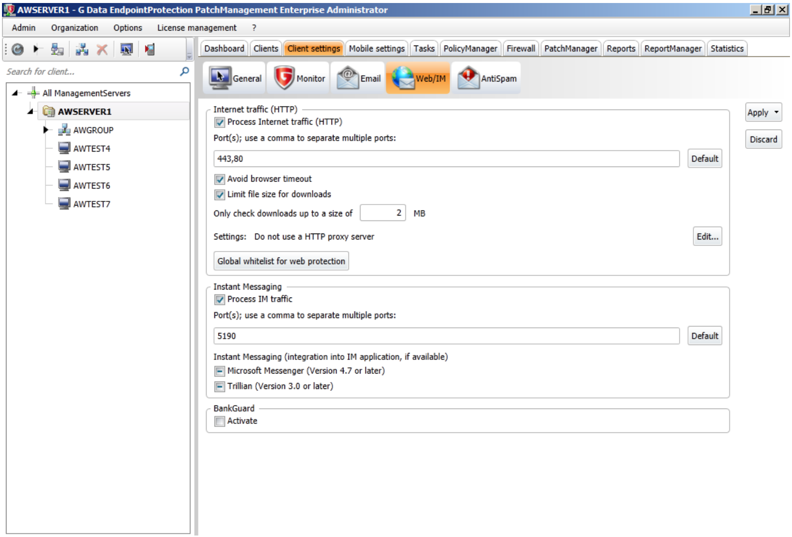
- **Protect Microsoft Outlook with an integrated plugin**: Activation of this function inserts a new function in the client's Outlook program under the **Tools** menu, called **Check folder for viruses**. Regardless of the G Data Administrator settings, an individual client user can scan the currently 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 summarized. 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.

Port monitoring

By default, the standard ports for POP3 (110), IMAP (143) and SMTP (25) are monitored. If your system's port settings are different, you can customize the settings accordingly.

Web/IM

The Web/IM panel allows you to define in-depth scan settings for internet traffic, instant messaging and online banking. If you do not want to check Internet content, the **Virus monitor** engages anyway when a user accesses 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.



Internet traffic (HTTP)

☑ Process Internet traffic (HTTP)

Port(s); use a comma to separate multiple ports: 443,80

☑ Avoid browser timeout

☑ Limit file size for downloads

Only check downloads up to a size of 2 MB

Settings: Do not use a HTTP proxy server

Instant Messaging

☑ Process IM traffic

Port(s); use a comma to separate multiple ports: 5190

Instant Messaging (integration into IM application, if available)

☐ Microsoft Messenger (Version 4.7 or later)

☐ Trillian (Version 3.0 or later)

BankGuard

☐ Activate

Internet traffic (HTTP)

- **Process Internet traffic (HTTP)**: HTTP web content is checked for viruses while browsing. Infected web content is not run at all and infected pages are not displayed. If the network is using a proxy to access the Internet, the server port the proxy is using must be entered. **Web content control** (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, there will be a certain amount of latency, depending on the data traffic. It is possible for an error message to appear in the Internet browser because the browser does not receive data immediately. This error message can be suppressed by enabling Avoid browser timeout. As soon as all browser data have been checked for viruses, they will be transmitted to the Internet browser.
- **Limit file size for downloads**: You can disable the HTTP check for web content that is too large. The contents will still be monitored by the virus monitor to check if suspected malicious routines become active. The advantage of enabling the size limit is that there are no delays caused by virus checks when downloading large files.
- **Global whitelist for web protection**: Exclude certain web sites from the web protection check.

Instant Messaging

- **Process IM traffic**: G Data software can prevent infected viruses and other malware from spreading via Instant Messaging. If the Instant Messaging applications are not using their standard ports, enter the corresponding ports under **Port (s)**.
- **Instant Messaging (integration into IM application, if available)**: If you use Microsoft Messenger (version 4.7 or later) or Trillian (version 3.0 or later), you can make an extra context menu available in the IM application, in which you can directly check suspicious files for viruses.

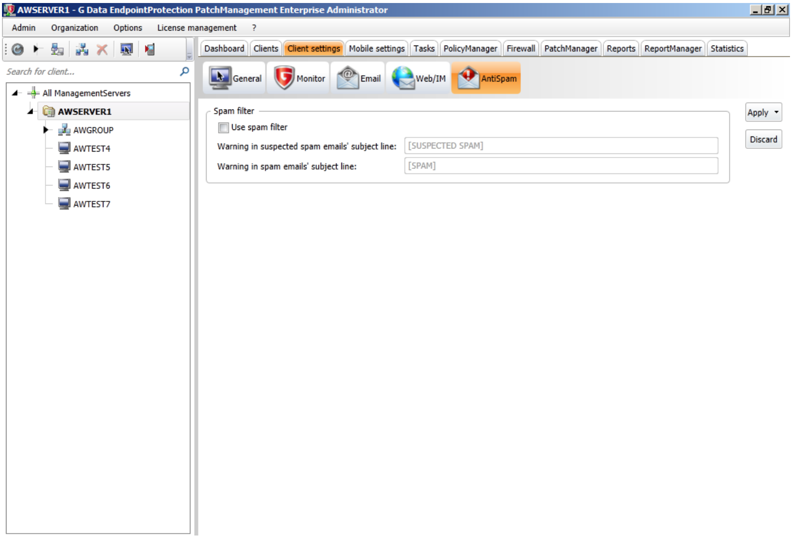
BankGuard

Banking trojans are becoming an ever greater threat. The BankGuard technology secures online banking by checking the validity of network libraries, to make sure the browser is not being manipulated by a banking trojan. This proactive protection works in more than 99% of the cases and even protects from unknown trojans. BankGuard should be activated for all clients that use Internet Explorer or Firefox.

AntiSpam

If you check the option **Use spam filter,** client email traffic will be checked for possible spam mails. You can define a warning that will be added to the subject line when an email is identified as spam or falls under suspicion of being spam.

> You or the user can define a rule in the client's email software to automatically move mail that has *[Spam]* in the subject line to a special folder for spam and junk mail.



Spam filter

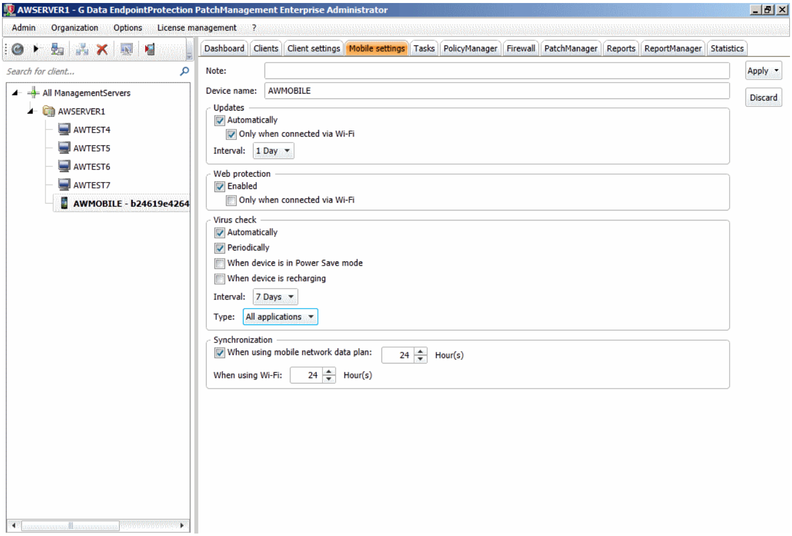
☐ Use spam filter

Warning in suspected spam emails' subject line: [SUSPECTED SPAM]

Warning in spam emails' subject line: [SPAM]

Mobile settings

If you have selected a mobile client in the **client management area**, you can manage its settings on the Mobile settings tab.



Note:

Device name: AWMOBILE

Updates

☑ Automatically

☑ Only when connected via Wi-Fi

Interval: 1 Day

Web protection

☑ Enabled

☐ Only when connected via Wi-Fi

Virus check

☑ Automatically

☑ Periodically

☐ When device is in Power Save mode

☐ When device is recharging

Interval: 7 Days

Type: All applications

Synchronization

☑ When using mobile network data plan: 24 Hour(s)

When using Wi-Fi: 24 Hour(s)

- **Note**: Enter any notes or remarks that apply to this mobile client.
- **Device name**: The name of the mobile device.

Updates

- **Automatically**: You can configure whether the mobile client software should be updated automatically or manually. If you choose automatic updates, you can set the interval and limit the updates to happen only when there is Wi-Fi connectivity.

Web protection

- **Web protection**: Enable Web protection to protect mobile clients when they access the internet. The G Data Monitor protection can be enabled for all web traffic or only when there is Wi-Fi connectivity.

Virus check

- **Automatically**: The virus check is carried out automatically and doesn't need to be initiated by the user.
- **Periodically**: The virus check can be scheduled. Tick the checkbox Periodically and specify the **Interval.**
- **When device is in Power Save mode**: Allow a virus check while the client is in battery saving mode.
- **When device is recharging**: Allow a virus check while the client is being charged.
- **Type**: Scan **all applications** or only **installed applications**.

Synchronization

The Synchronization option defines if and when the virus signatures should be updated. You can set an interval and configure updates to happen only when there is Wi-Fi connectivity or also using a mobile network data plan.

Tasks

In the Tasks module, you can define tasks, or jobs, for the G Data Clients. All tasks generated on the G Data ManagementServer are referred to as jobs. There are two different job types: single jobs and periodic jobs. Single jobs are performed once at a specific time; for the periodic jobs, a schedule is defined. You can define as many different jobs as you would like. For performance reasons, it generally makes sense that jobs do not overlap.

In the Tasks area, jobs be sorted according to the following criteria by simply clicking on the respective column header. The column according to which the list is currently sorted is indicated by a small arrow symbol.

- **Name**: The name specified by you for the job. You can enter a name of any length.
- **Computer**: You will find the name of the corresponding clients here. You can only define jobs for enabled clients.
- **Group**: If you assign a job to a group, the group name appears in the overview list rather than the individual computers.
- **Status**: The Status column shows the status or the results of a job displayed in plain text. For example, you can see whether the job has just run or has been completed, and also find out whether or not any viruses were found.
- **Last run**: When the respective job was last run.
- **Time interval**: This column shows the cycle with which the job will be repeated according to the defined schedule.
- **Analysis scope**: Find out which media (e.g. local hard disks) the analysis includes.

To manage tasks, you can use the following options from the toolbar above the task list:

Refresh: Update the view and loads the current job list from the G Data ManagementServer.

Delete: Delete all highlighted jobs.

Single scan job: Define a single scan job for individual computers or computer groups. In the configuration dialog, the time, scope, and additional scan settings can be defined on their respective 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). You can now change the scan job settings to what you want.

Periodic scan job: Define a periodic scan job for individual computers or computer groups. In the configuration dialog, schedule, 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). You can now change the scan job settings to what you want.

Backup job: Define a backup job for individual computers or computer groups. For more information about backup jobs, see the chapter **Backup jobs**. The Backup function is only available as part of the Enterprise **solutions**.

Restore: This function allows you to restore backups to clients or groups. The Restore function is only available as part of the Enterprise **solutions**.

Software recognition job: List software and patches that have been installed on clients or groups. For more information about software recognition jobs, see the chapter **Software recognition jobs**. The Software recognition function is only available as part of the optional PatchManagement **module**.

Software distribution job: Schedule software and patch distribution. For more information about software distribution jobs, see the chapter **Software distribution jobs**. The Software distribution function is only available as part of the optional PatchManagement **module**.

Run now: Re-run single scan jobs which have already been run or cancelled. For periodic scan jobs, this function runs the job immediately, regardless of schedule.

Logs: View the logs relating to a particular client's jobs.

Display all tasks

Display only scan jobs

Display only backup jobs (only available as part of the Enterprise **solutions**)

Display only restore jobs (only available as part of the Enterprise **solutions**)

Display only software recognition jobs (only available as part of the optional PatchManagement **module**)

Display only software distribution jobs (only available as part of the optional PatchManagement **module**)

Display only rollback jobs (only available as part of the optional PatchManagement **module**)

Display only single scan jobs

Display only periodic scan jobs

Display only pending scan jobs

Display only 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.

Menu bar

When the Tasks module is selected, an additional menu entry named **Tasks** becomes available in the menu bar. The following options are included:

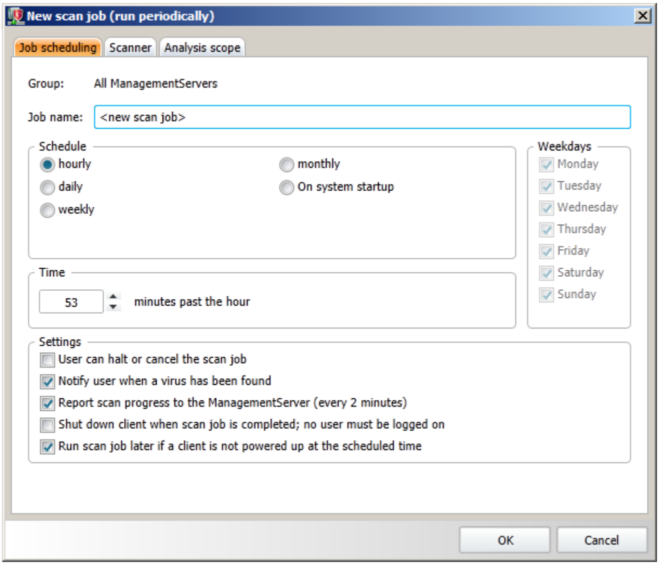
- **View**: Select whether you would like to display all jobs or only scan jobs, backup jobs, restore jobs, software recognition jobs, software distribution jobs, rollback jobs, single scan jobs, periodic scan jobs, pending scan jobs, or completed scan jobs (depending on your product version). For scan jobs that were defined for a group of clients, you can decide whether detailed information about all clients should be displayed by ticking **Display group jobs in detail**.
- **Run now**: Re-run single scan jobs which have already been run or cancelled. For periodic scan jobs, this function runs the job immediately, regardless of schedule.

- **Cancel**: Cancel a running job.
- **Delete**: Delete selected jobs.
- **New**: Create a single scan job or a periodic scan job. You can also generate a backup job, restore job, software recognition job, or software distribution job (depending on your product version).

Scan jobs

Job scheduling

Use the **Job name** field to specify which name the scan job should have. You can enter meaningful names here such as *Archive Scan* or *Monthly Scan* to clearly label the job so that it can be found again in the table overview. Permissions can be granted to the users for pausing or aborting the job via the system tray context menu. You can enable **Report scan progress to the ManagementServer** to report the status of a scan process to the server every two minutes. **Shut down client when scan job is completed** provides another way to help reduce your administrative load. If a computer is not switched on at the scheduled time of a periodic scan job, the scan job can be started later by ticking **Run scan job later if a client is not powered up at the scheduled time**.



Group: All ManagementServers

Job name: <new scan job>

Schedule
● hourly
○ daily
○ weekly
○ monthly
○ On system startup

Weekdays
☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday
☑ Sunday

Time
53 minutes past the hour

Settings
□ User can halt or cancel the scan job
☑ Notify user when a virus has been found
☑ Report scan progress to the ManagementServer (every 2 minutes)
□ Shut down client when scan job is completed; no user must be logged on
☑ Run scan job later if a client is not powered up at the scheduled time

For periodic scan jobs, this tab also 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 scan each time your computer is restarted. For **Daily** jobs, you can specify under **Weekdays** on which specific days of the week the job should be carried out.

> 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

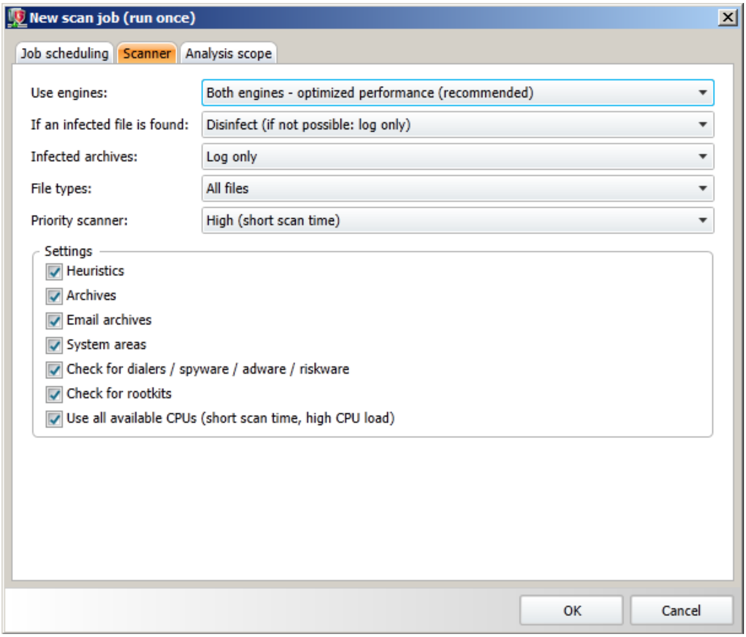
The Scanner tab shows the settings with which the scan job will be executed. The following options are available:

- **Use engines**: The G Data software works with two independently operating virus scanning engines. Using both engines guarantees optimum results for preventing viruses. Using just one engine may have performance advantages. We recommend the setting **Both engines - performance optimized**. In this scenario, both virus scanners cooperate to achieve optimized detection with a minimized scanning duration.
- **If an infected file is found**: Specify what should happen if an infected file is detected. There are various options that may or may not be suitable, depending on what the client computer is used for. By setting **Move file to quarantine**, an infected file is moved to a special directory that is created by G Data ManagementServer. Infected files are encrypted there so that potential 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 **Security Labs**.
- **Infected archives**: Specify here how infected **archives** are to be treated. 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 the virus check should have high priority on the client (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). Which priority to choose mostly depends on the point of time at which the virus check will be carried out.
- **Settings**: Specify the additional virus analyses you want the G Data software to perform. The default options are the recommended ones, but 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 signature databases, but also on characteristics that are typical of most viruses. Heuristics can generate a false alarm in rare instances.
    - **Archives**: Checking compressed data in archives is very time consuming and can generally be skipped if **G Data monitor** is active on the client. 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 archives**: Checking email archives is very time consuming and can generally be omitted if **G Data monitor** or the Outlook plug-in is enabled on the client. While accessing the archive, the monitor will detect viruses and will automatically take care of them. Nevertheless, during regular checks of the computer outside the actual usage times, checking of email archives should also take place.
    - **System areas**: The system areas of your computer (boot sectors, master boot record etc.) should not be excluded from the virus check as some malware stores itself there.

- **Check for dialers / spyware / adware / riskware**: You can use the G Data software to check your system for dialers and other malware programs (spyware, adware, riskware). This includes programs that establish unrequested expensive Internet connections and are potentially every bit as damaging as a virus in terms of economical impact. Spyware, for example, can record end user surfing habits or even all keyboard entries (including passwords) without the user knowing and, at the next opportunity, forward them to unknown recipients over the Internet.
- **Check for rootkits**: A rootkit attempts to evade conventional virus detection methods. You can use this function to specifically search for rootkits, without checking all hard drives and files.
- **Use all available CPUs**: 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 only be used if the scan job is executed at times when the system is not regularly used (e.g. at night).



New scan job (run once)

Use engines: Both engines - optimized performance (recommended)

If an infected file is found: Disinfect (if not possible: log only)

Infected archives: Log only

File types: All files

Priority scanner: High (short scan time)

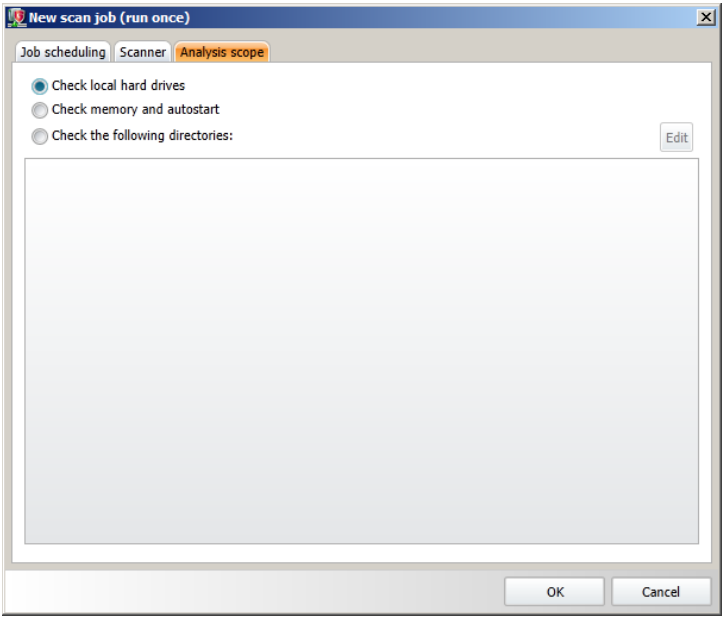
Settings

☑ Heuristics
☑ Archives
☑ Email archives
☑ System areas
☑ Check for dialers / spyware / adware / riskware
☑ Check for rootkits
☑ Use all available CPUs (short scan time, high CPU load)

Analysis scope

You can limit the virus check 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. The folder selection window allows you to pick folders from both the local PC and network clients.

Special note for Linux file servers: when selecting directory exceptions, the root drive (/) and all shares are listed. This way, drive, directory, and file exceptions can be created.



New scan job (run once)

Job scheduling | Scanner | Analysis scope

● Check local hard drives
○ Check memory and autostart
○ Check the following directories:

Backup jobs

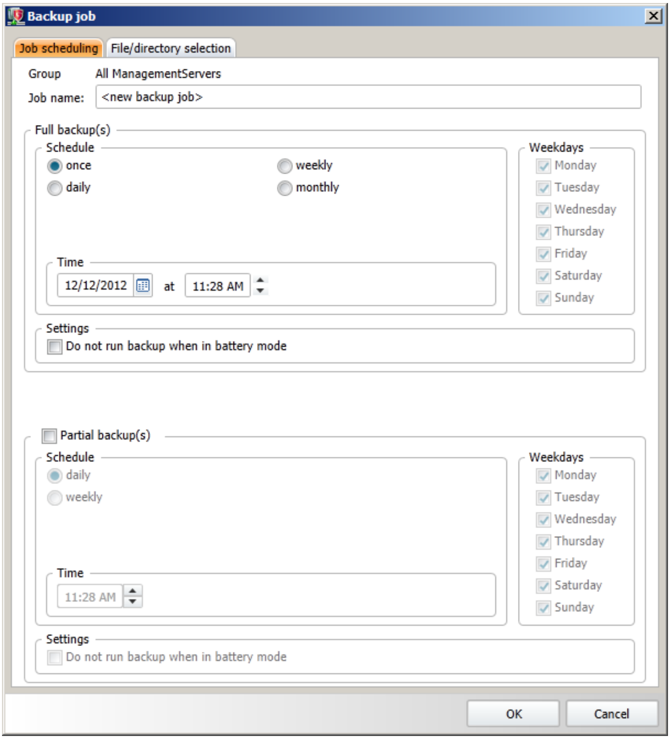
The Backup function is only available as part of the Enterprise **solutions**.

Job scheduling

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. You can set up **full backups** or **partial backups** (differential) at defined times. A partial backup only saves files that have been altered since the last full or partial backup. In this case, the backup job will need less time, but restoring a partial backup takes longer because it will have to be rebuilt from multiple backup files.

Enable **Do not run backup when in battery mode** to prevent burdening mobile computers running in battery mode with a backup job. The backup will be made up as soon as the client is connected to a power supply. For **Daily** jobs, you can specify under **Weekdays** on which specific days of the week the job should be carried out.

Provided nothing else is indicated in the **Server settings**, backups will be saved on the ManagementServer 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 G Data Administrator.



Group All ManagementServers

Job name: <new backup job>

Full backup(s)

Schedule

● once ○ weekly

○ daily ○ monthly

Time

12/12/2012 at 11:28 AM

Weekdays

☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday
☑ Sunday

Settings

□ Do not run backup when in battery mode

□ Partial backup(s)

Schedule

● daily

○ weekly

Time

11:28 AM

Weekdays

☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday
☑ Sunday

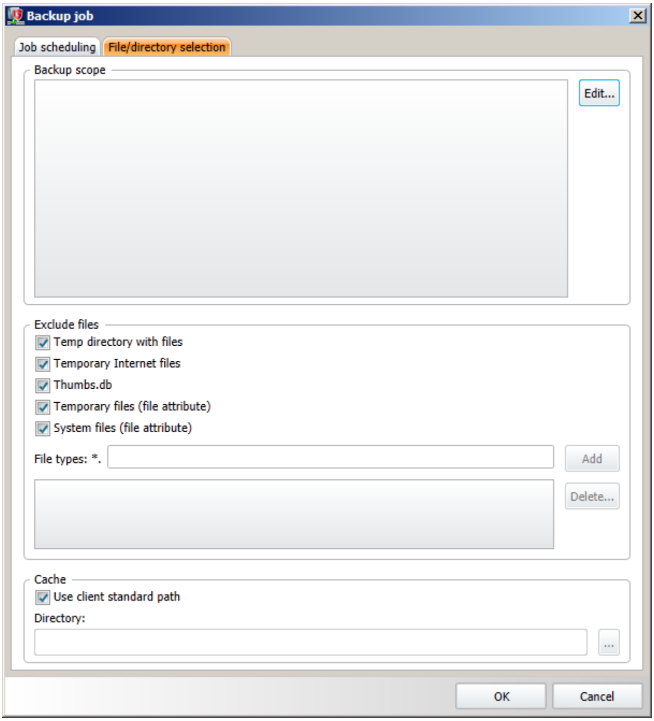
Settings

□ Do not run backup when in battery mode

File/directory selection

The File/directory selection tab lets you select which folders from which clients or groups will be backed up. Under **Backup scope**, add folders from any of the clients. **Exclude files** allows you to define files and folders to be excluded from the backup. There are several general options, such as **Temporary internet Files** and **Thumbs.db**, but you can also define custom file types by adding their extension to the file type list.

If the generated backup should be saved in a particular directory prior to transmission to the ManagementServer, this 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.



Exclude files

☑ Temp directory with files

☑ Temporary Internet files

☑ Thumbs.db

☑ Temporary files (file attribute)

☑ System files (file attribute)

File types: *.

Cache

☑ Use client standard path

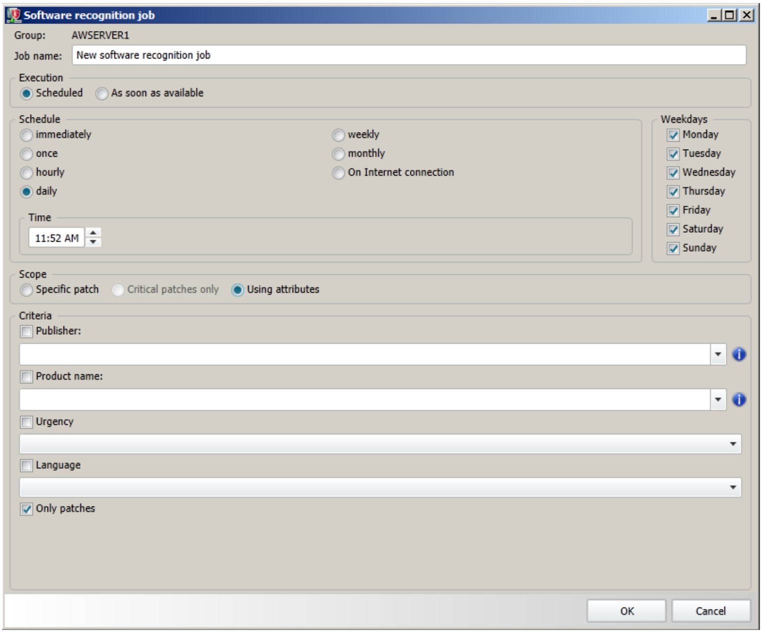
Directory:

Software recognition jobs

The Software recognition function is only available as part of the optional PatchManagement **module**.

Software recognition jobs can be planned to check clients or groups for applicable **patches**. The recognition job can be **scheduled** or run **as soon as available**. Additionally, you can define the scope to be limited to specific patches or to search using attributes.

Enter the attributes of the software that you want to recognise. To add a specific attribute (Publisher, Product name, Urgency, Language) as a search criterium, tick the checkbox and enter the search term. This way you can look for software only from a specific publisher or only specific versions. Wildcards like "?" and "*" can be used to filter.



Software recognition job

Group: AWSERVER1

Job name: New software recognition job

Execution

● Scheduled ○ As soon as available

Schedule

○ immediately
○ once
○ hourly
● daily
○ weekly
○ monthly
○ On Internet connection

Time

11:52 AM

Weekdays

☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday
☑ Sunday

Scope

○ Specific patch ○ Critical patches only ● Using attributes

Criteria

□ Publisher:

□ Product name:

□ Urgency

□ Language

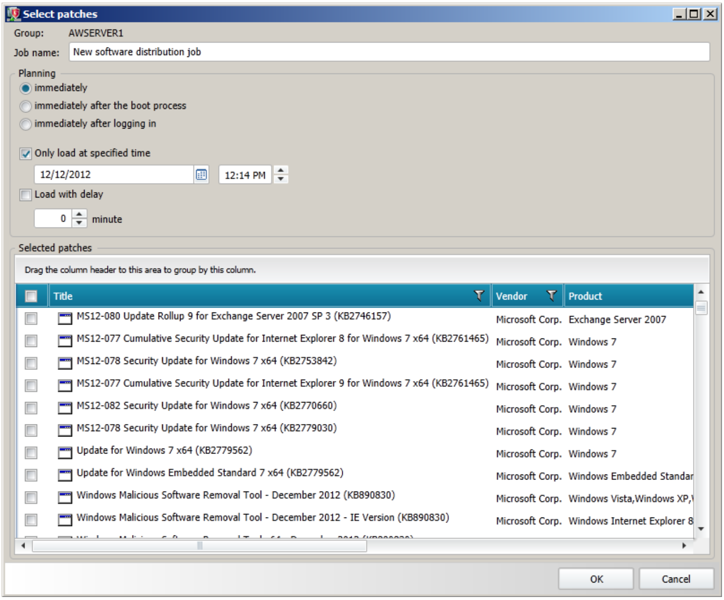
☑ Only patches

Software distribution jobs

The Software distribution function is only available as part of the optional PatchManagement **module**.

To distribute **applicable patches** to clients or groups, you can define a software distribution job. By ticking the option **Only load at a specified time**, you can schedule the job. The actual software distribution can be carried out **immediately**, **immediately after the boot process**, or **immediately after logging in**. Additionally, you can schedule a delay in starting the job. That way, the boot process and distribution job won't influence client performance at the same time.

To uninstall previously deployed patches, you can plan a rollback job through the PatchManager **Overview** panel, or directly by right-clicking on the respective distribution job in the Tasks overview and choosing **Rollback**.



Group: AWSERVER1

Job name: New software distribution job

Planning

● immediately

○ immediately after the boot process

○ immediately after logging in

☑ Only load at specified time

12/12/2012 12:14 PM

□ Load with delay

0 minute

Selected patches

Drag the column header to this area to group by this column.

□	Title	Vendor	Product
□	MS12-080 Update Rollup 9 for Exchange Server 2007 SP 3 (KB2746157)	Microsoft Corp.	Exchange Server 2007
□	MS12-077 Cumulative Security Update for Internet Explorer 8 for Windows 7 x64 (KB2761465)	Microsoft Corp.	Windows 7
□	MS12-078 Security Update for Windows 7 x64 (KB2753842)	Microsoft Corp.	Windows 7
□	MS12-077 Cumulative Security Update for Internet Explorer 9 for Windows 7 x64 (KB2761465)	Microsoft Corp.	Windows 7
□	MS12-082 Security Update for Windows 7 x64 (KB2770660)	Microsoft Corp.	Windows 7
□	MS12-078 Security Update for Windows 7 x64 (KB2779030)	Microsoft Corp.	Windows 7
□	Update for Windows 7 x64 (KB2779562)	Microsoft Corp.	Windows 7
□	Update for Windows Embedded Standard 7 x64 (KB2779562)	Microsoft Corp.	Windows Embedded Standar
□	Windows Malicious Software Removal Tool - December 2012 (KB890830)	Microsoft Corp.	Windows Vista,Windows XP,\
□	Windows Malicious Software Removal Tool - December 2012 - IE Version (KB890830)	Microsoft Corp.	Windows Internet Explorer 8

PolicyManager

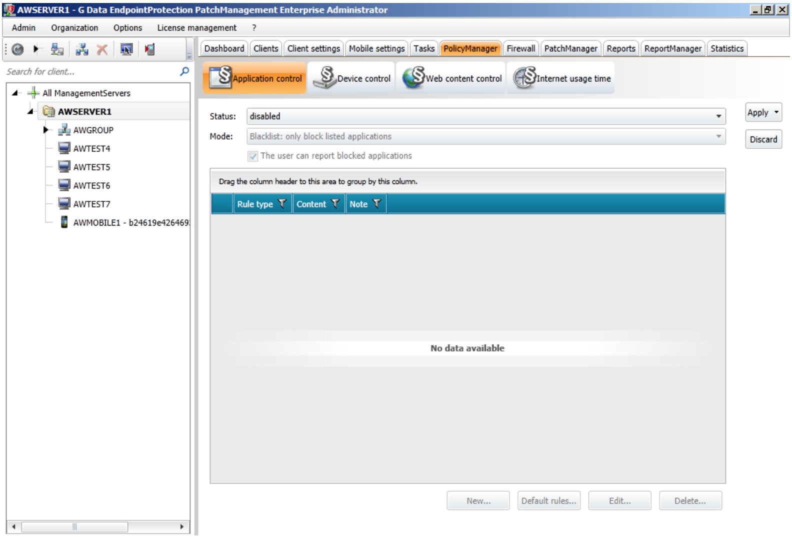
The PolicyManager module is only available as part of the EndpointProtection Enterprise and EndpointProtection Business **solutions**.

PolicyManager includes application, device, and web content control as well as monitoring of Internet usage time. These functions allow comprehensive implementation of company guidelines for the use of internal company PCs. Using the PolicyManager a system administrator can define 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.

Application control

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

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



AWSERVER1 - G Data EndpointProtection PatchManagement Enterprise Administrator

Status: disabled

Mode: Blacklist: only block listed applications

☑ The user can report blocked applications

Drag the column header to this area to group by this column.

Rule type	Content	Note

No data available

Create new rule

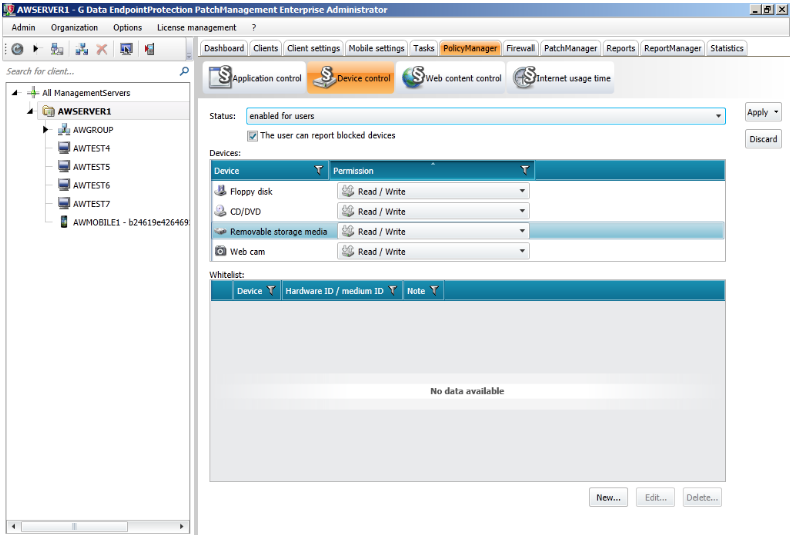
A new rule can be defined using the **New...** button. Rules are categorised as one of three types:

- **Vendor**: 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, using which the manufacturer information can be read and imported.

- **File**: Block or allow specific program files for the particular client. You can either enter the file name to generally forbid or allow access to files with this name or click the button **Determine file properties...** to define a file 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**: 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. Users can be prevented from using USB sticks or other external storage media utilizing the USB port, as well as CD/DVD drives and even webcams.



Status: enabled for users

☑ The user can report blocked devices

Devices:

Device	Permission
Floppy disk	Read / Write
CD/DVD	Read / Write
Removable storage media	Read / Write
Web cam	Read / Write

Whitelist:

Device	Hardware ID / medium ID	Note

No data available

Under **Status** you can specify whether the limitations should apply to all users of the client in question (including administrators) 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 using the whitelist settings, you can allow access for a client, with certain limitations, to devices to which you had previously limited access in some way or another (**Read** / **Deny access**). When you click the **New...** button a dialog window opens in which devices with usage limitations are displayed. If you then click on **[...]**, you can permit exceptions for certain devices.

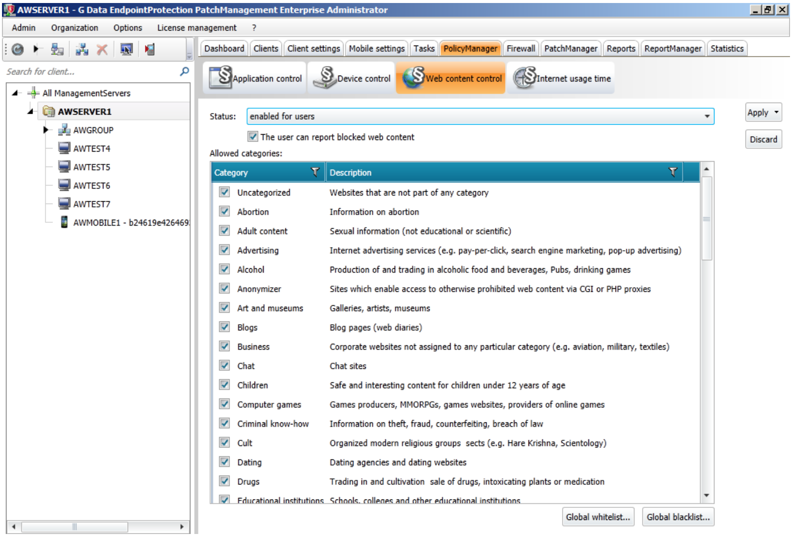
- **Use medium ID**: Specify that only certain CDs or DVDs can be used with a CD/DVD drive, such as company presentations on CD.
- **Use hardware ID**: Specify that only certain USB sticks may be used. With whitelisting based on hardware ID for individual storage devices, the network administrator has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

To determine a medium ID or hardware ID, select the client in the **Select Source** field in the dialogue box **Read hardware ID / medium ID**. 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 G Data Administrator is installed. For this, the medium must be connected with or inserted in the corresponding PC.

Web content control

Web content control is used to provide users with Internet access within the scope of their duties while preventing visiting non-desirable websites or websites in particular subject areas. You can select or block certain areas by checking or unchecking a checkbox for the client in question. The categories 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 (including administrators) or only to users who do not have administrator rights on the client computer.



Status: enabled for users

☑ The user can report blocked web content

Allowed categories:

Category	Description
☑ Uncategorized	Websites that are not part of any category
☑ Abortion	Information on abortion
☑ Adult content	Sexual information (not educational or scientific)
☑ Advertising	Internet advertising services (e.g. pay-per-click, search engine marketing, pop-up advertising)
☑ Alcohol	Production of and trading in alcoholic food and beverages, Pubs, drinking games
☑ Anonymizer	Sites which enable access to otherwise prohibited web content via CGI or PHP proxies
☑ Art and museums	Galleries, artists, museums
☑ Blogs	Blog pages (web diaries)
☑ Business	Corporate websites not assigned to any particular category (e.g. aviation, military, textiles)
☑ Chat	Chat sites
☑ Children	Safe and interesting content for children under 12 years of age
☑ Computer games	Games producers, MMORPGs, games websites, providers of online games
☑ Criminal know-how	Information on theft, fraud, counterfeiting, breach of law
☑ Cult	Organized modern religious groups sects (e.g. Hare Krishna, Scientology)
☑ Dating	Dating agencies and dating websites
☑ Drugs	Trading in and cultivation sale of drugs, intoxicating plants or medication
☑ Educational institutions	Schools, colleges and other educational institutions

Global whitelist

Using the **Global whitelist**, it is possible to ensure that certain websites are allowed company-wide across the entire network, regardless of any settings that have been made under **Allowed categories**. 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.

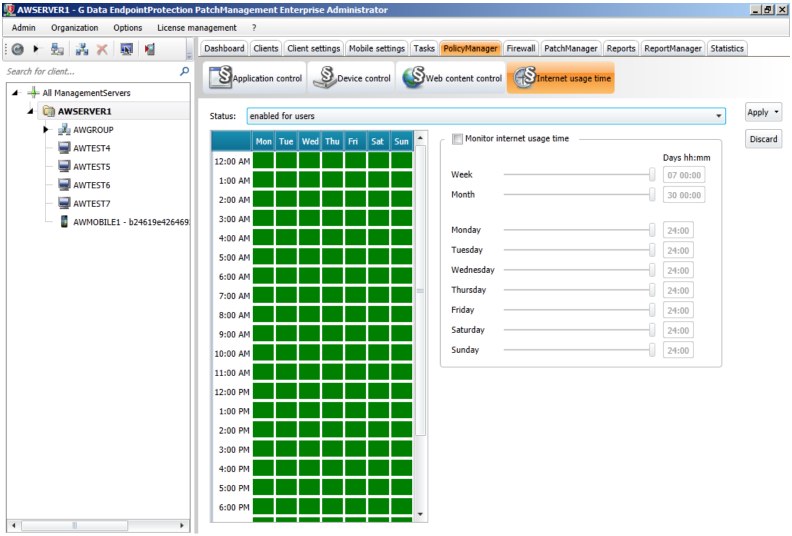
Global blacklist

Using the **Global blacklist**, it is possible to ensure that certain websites are blocked company-wide across the entire network, regardless of any settings that have been made under **Allowed categories**. 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

On the Internet usage time panel, general use of the Internet can be restricted to certain times. Setting up 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 (including administrators) or only to users who do not have administrator rights on the client computer. On the right side, you can use the available controls to specify the quota available for Internet usage. 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 used. 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.



Status: enabled for users

□ Monitor internet usage time

	Days hh:mm
Week	07 00:00
Month	30 00:00
Monday	24:00
Tuesday	24:00
Wednesday	24:00
Thursday	24:00
Friday	24:00
Saturday	24:00
Sunday	24:00

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 lockout 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: **Allow time** and **Block time**. 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.

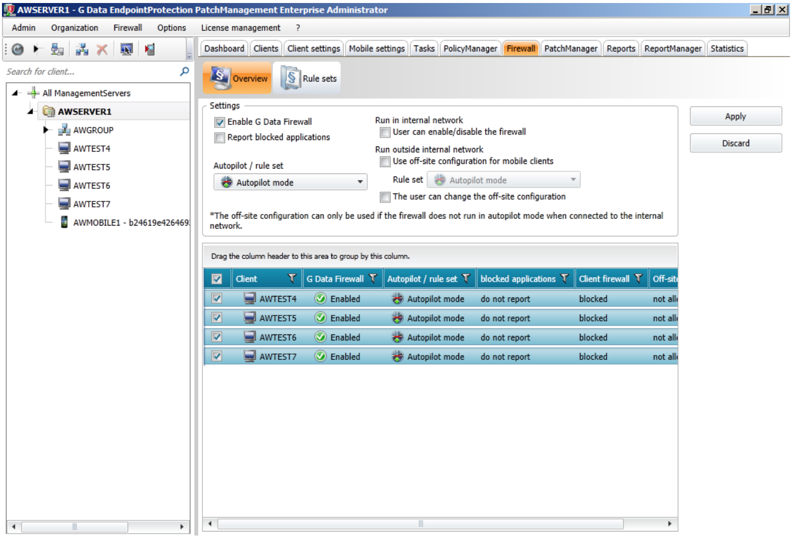
Firewall

The Firewall module is only available as part of the ClientSecurity (Enterprise/Business) and EndpointProtection (Enterprise/ Business) **solutions**.

The Firewall allows you to centrally administer the firewall for clients and 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

There are two fundamentally different modes for operating the firewall. When the firewall is running on **Autopilot**, it is preconfigured by G Data and carries out its tasks in the background, without interrupting the user. In Autopilot mode, the firewall optimizes its rule sets autonomously over time. The second mode, **Rule sets**, allows you to define individual firewall rules and rule sets for different computers.



Settings

☑ Enable G Data Firewall
☐ Report blocked applications

Autopilot / rule set: Autopilot mode

Run in internal network
☐ User can enable/disable the firewall

Run outside internal network
☐ Use off-site configuration for mobile clients

Rule set: Autopilot mode

☐ The user can change the off-site configuration

*The off-site configuration can only be used if the firewall does not run in autopilot mode when connected to the internal network.

Drag the column header to this area to group by this column.

☑	Client	G Data Firewall	Autopilot / rule set	blocked applications	Client firewall	Off-sit
☑	AWTEST4	Enabled	Autopilot mode	do not report	blocked	not all
☑	AWTEST5	Enabled	Autopilot mode	do not report	blocked	not all
☑	AWTEST6	Enabled	Autopilot mode	do not report	blocked	not all
☑	AWTEST7	Enabled	Autopilot mode	do not report	blocked	not all

All client computers or clients in a selected group are displayed in the overview. This enables you to see at a glance how the client firewall has been configured and to make changes directly. The list contains the following data:

- **Client**: Client computer name. You can use the icons being displayed to tell if the client software is installed on this client.
- **G Data Firewall**: Here, you can tell if the firewall on the client is installed, enabled or disabled.
- **Autopilot / Rule set**: Shows which rule set has been applied to the client.
- **Blocked applications**: Displays whether blocked applications are reported or not.
- **Client firewall**: Shows whether users can enable and disable the firewall.

- **Off-site configuration**: If you enable off-site configuration, the user can manage and configure the firewall settings on this client how he wishes, as long as he is not connected to the G Data 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 any client. This will open a context menu with the following options:

- **Create rule set**: Switch to the **Rule sets** area to define specific rules for your client firewall.
- **Edit rule set**: Switch to the Rule sets area to modify existing rules for your client firewall.
- **Install G Data Firewall**: Install the firewall centrally on enabled client computers and subsequently administer them.
- **Uninstall G Data Firewall**: Uninstall the client's firewall.

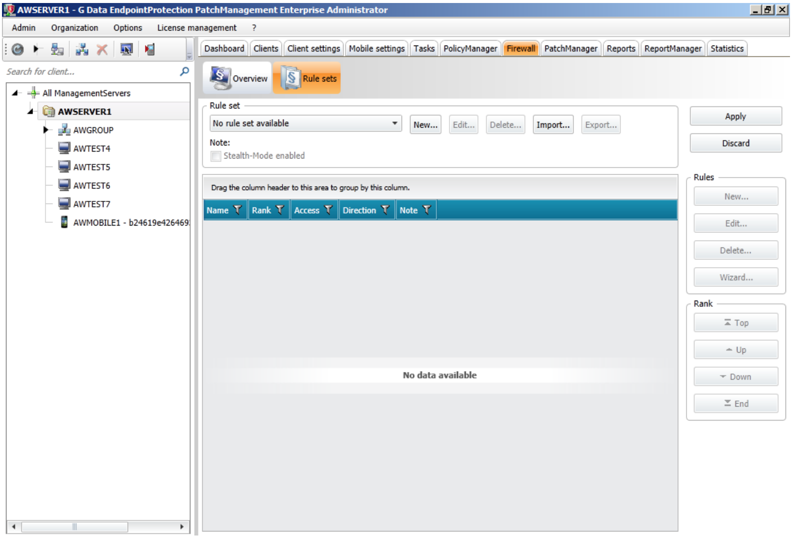
Firewall settings

- **Enable Firewall**: Enabled the firewall for the selected client or group. If you uncheck the box, the firewall is disabled.
- **Report blocked applications**: If the client computer is connected to the G Data ManagementServer, the system administrator will be notified in the **Reports** module when applications have been blocked by the client firewall.
- **User can enable/disable the firewall**: As network administrator, 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 only be enabled for competent users.
- **Use off-site configuration for mobile clients**: In the off-site configuration, firewall rule sets for your company network are automatically replaced by default off-site rule sets. This enables mobile computers to be optimally protected whenever they are outside of the G Data ManagementServer network. As soon as the mobile computer is reconnected to the G Data ManagementServer network, these default rule sets are automatically replaced by the rule sets that apply to that particular client within your network.

- **The user can change the off-site configuration**: Allow users to configure their firewall when they are outside of the network. As soon as the mobile computer is reconnected to the G Data ManagementServer, the changes made will be replaced with the rules put in place by the network administrator for this client. The off-site 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

On the Rule sets panel you can create special rules for different networks. These rules can then be grouped together to form a rule set.

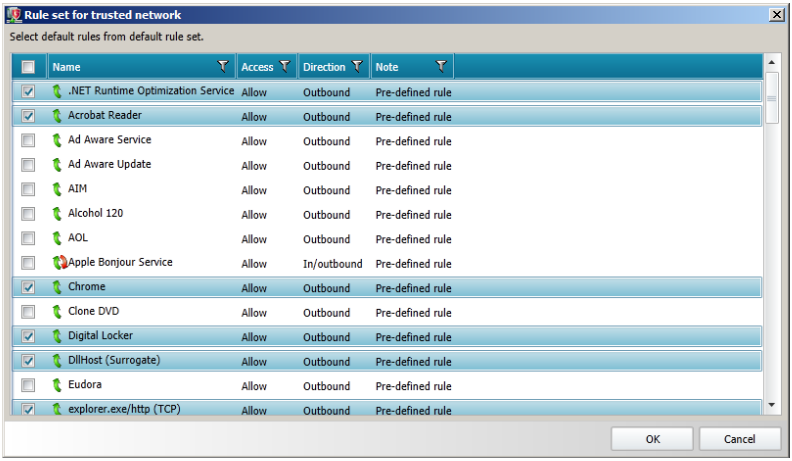


Rule set: No rule set available

□ Stealth-Mode enabled

New rule set

- **New**: Create a new rule set for a network
- **Stealth mode** blocks requests to the computer that try to verify a port's accessibility. This makes it difficult for attackers to obtain system information.



Rule set for trusted network

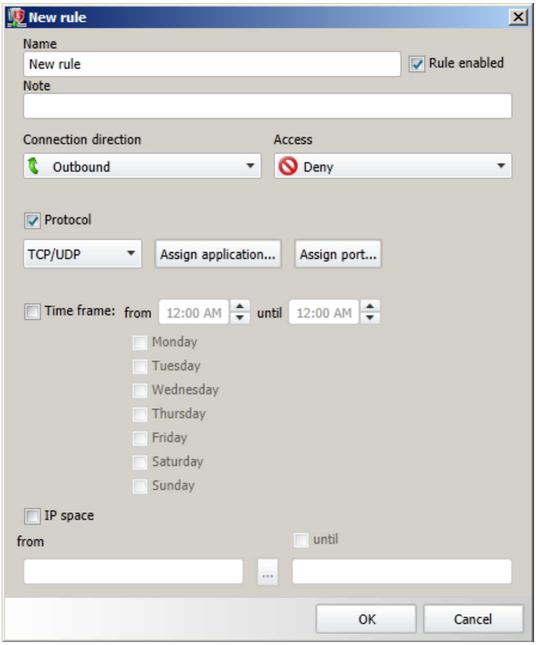
Select default rules from default rule set.

□	Name	Access	Direction	Note
☑	.NET Runtime Optimization Service	Allow	Outbound	Pre-defined rule
☑	Acrobat Reader	Allow	Outbound	Pre-defined rule
□	Ad Aware Service	Allow	Outbound	Pre-defined rule
□	Ad Aware Update	Allow	Outbound	Pre-defined rule
□	AIM	Allow	Outbound	Pre-defined rule
□	Alcohol 120	Allow	Outbound	Pre-defined rule
□	AOL	Allow	Outbound	Pre-defined rule
□	Apple Bonjour Service	Allow	In/outbound	Pre-defined rule
☑	Chrome	Allow	Outbound	Pre-defined rule
□	Clone DVD	Allow	Outbound	Pre-defined rule
☑	Digital Locker	Allow	Outbound	Pre-defined rule
☑	DllHost (Surrogate)	Allow	Outbound	Pre-defined rule
□	Eudora	Allow	Outbound	Pre-defined rule
☑	explorer.exe/http (TCP)	Allow	Outbound	Pre-defined rule

New rule/Edit rule

- **Name**: For pre-defined and automatically generated rules, this field displays the program name to which the relevant rule applies.
- **Rule enabled**: Disable a rule without actually deleting it.
- **Note**: This indicates how the rule was created. **Pre-defined rule** is listed next to preset rules; **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.
- **Connection direction**: With Direction, you specify if the selected rule applies to inbound or outbound connections, or both.
- **Access**: Allowed or denied access for the program within this rule set.
- **Protocol**: 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 (**Assign application**). Similarly, you can use the **Assign port** button to specify the ports that you do or do not wish to use.
- **Time frame**: Set up time-related access to network resources to ensure, for example, that the network can only be accessed during a normal working day and is blocked at all other times.

- **IP 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.



New rule

Name: New rule

☑ Rule enabled

Note:

Connection direction: Outbound

Access: Deny

☑ Protocol

TCP/UDP

□ Time frame: from 12:00 AM until 12:00 AM

□ Monday
□ Tuesday
□ Wednesday
□ Thursday
□ Friday
□ Saturday
□ Sunday

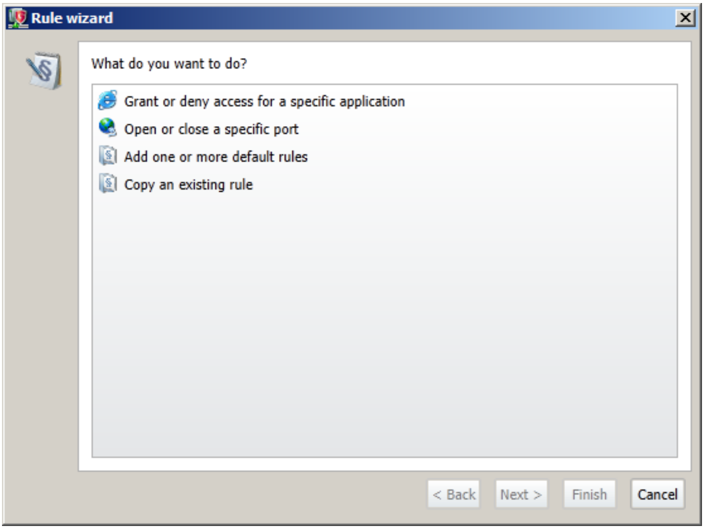
□ IP space

from

□ until

Rule wizard

The Rule wizard allows you to define additional specific rules for the relevant rule set or to modify existing rules. Using the Rule wizard, you change one or more rules in the selected rule set. 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 Internet.


Rule wizard
What do you want to do?
Grant or deny access for a specific application
Open or close a specific port
Add one or more default rules
Copy an existing rule
< Back
Next >
Finish
Cancel

The following actions are available in the Rule wizard:

- **Grant or deny access for a specific application**: 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 inbound connections, outbound connections, or both. This enables you, for example, to prevent your MP3 player software from forwarding data about your listening habits (outbound connections) or to ensure that program updates are not downloaded automatically (inbound connections).

- **Open or close a specific port**: The wizard provides the option of blocking ports completely or enabling them for a particular application only (e.g. CRM software).
- **Add one or more default rules**: Select which of the existing rules should be made default, so that they appear in each new rule set.
- **Copy an existing rule**

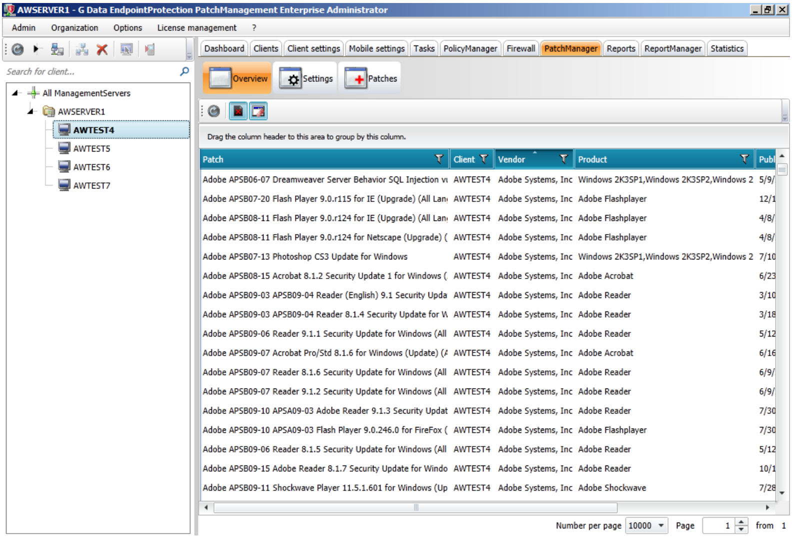
PatchManager

PatchManager is available as an optional module for users of the AntiVirus (Enterprise/Business), ClientSecurity (Enterprise/ Business) and EndpointProtection (Enterprise/Business) **solutions**.

PatchManager allows you to control patch deployment for all managed machines from one single interface. You can use PatchManager to list updates for software from Microsoft and other parties. Each patch can be checked for applicability, blacklisted, distributed or rolled back, grouped or individually.

Overview

The Overview panel provides a detailed view of patches and their deployment status within the network. The extensive list can be filtered to show whether clients have been provided with all relevant patches and allows you to directly schedule patch deployment.



Patch	Client	Vendor	Product	Publ
Adobe APSB06-07 Dreamweaver Server Behavior SQL Injection vu	AWTEST4	Adobe Systems, Inc	Windows 2K3SP1,Windows 2K3SP2,Windows 2	5/9/
Adobe APSB07-20 Flash Player 9.0.r115 for IE (Upgrade) (All Lan	AWTEST4	Adobe Systems, Inc	Adobe Flashplayer	12/1
Adobe APSB08-11 Flash Player 9.0.r124 for IE (Upgrade) (All Lan	AWTEST4	Adobe Systems, Inc	Adobe Flashplayer	4/8/
Adobe APSB08-11 Flash Player 9.0.r124 for Netscape (Upgrade) (	AWTEST4	Adobe Systems, Inc	Adobe Flashplayer	4/8/
Adobe APSB07-13 Photoshop CS3 Update for Windows	AWTEST4	Adobe Systems, Inc	Windows 2K3SP1,Windows 2K3SP2,Windows 2	7/10
Adobe APSB08-15 Acrobat 8.1.2 Security Update 1 for Windows (	AWTEST4	Adobe Systems, Inc	Adobe Acrobat	6/23
Adobe APSB09-03 APSB09-04 Reader (English) 9.1 Security Upda	AWTEST4	Adobe Systems, Inc	Adobe Reader	3/10
Adobe APSB09-03 APSB09-04 Reader 8.1.4 Security Update for W	AWTEST4	Adobe Systems, Inc	Adobe Reader	3/18
Adobe APSB09-06 Reader 9.1.1 Security Update for Windows (All	AWTEST4	Adobe Systems, Inc	Adobe Reader	5/12
Adobe APSB09-07 Acrobat Pro/Std 8.1.6 for Windows (Update) (A	AWTEST4	Adobe Systems, Inc	Adobe Acrobat	6/16
Adobe APSB09-07 Reader 8.1.6 Security Update for Windows (All	AWTEST4	Adobe Systems, Inc	Adobe Reader	6/9/
Adobe APSB09-07 Reader 9.1.2 Security Update for Windows (All	AWTEST4	Adobe Systems, Inc	Adobe Reader	6/9/
Adobe APSB09-10 APSA09-03 Adobe Reader 9.1.3 Security Updat	AWTEST4	Adobe Systems, Inc	Adobe Reader	7/30
Adobe APSB09-10 APSA09-03 Flash Player 9.0.246.0 for FireFox (	AWTEST4	Adobe Systems, Inc	Adobe Flashplayer	7/30
Adobe APSB09-06 Reader 8.1.5 Security Update for Windows (All	AWTEST4	Adobe Systems, Inc	Adobe Reader	5/12
Adobe APSB09-15 Adobe Reader 8.1.7 Security Update for Windo	AWTEST4	Adobe Systems, Inc	Adobe Reader	10/1
Adobe APSB09-11 Shockwave Player 11.5.1.601 for Windows (Up	AWTEST4	Adobe Systems, Inc	Adobe Shockwave	7/28

Number per page 10000 Page 1 from 1

The Overview panel lists all of the available patches, alphabetically, once per client. To effectively manage the list, several filtering options are available:

Refresh: refresh the list to take the latest changes into account.

Hide patches on the blacklist: hide patches that have been added to the blacklist.

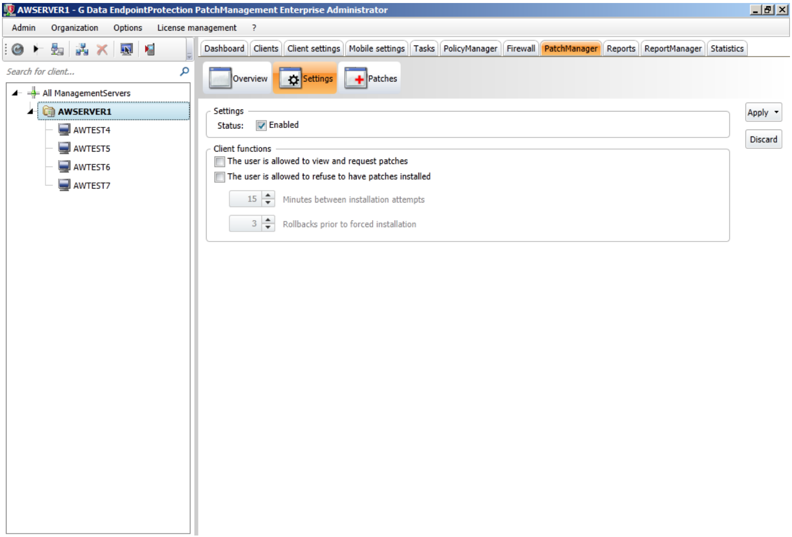
Display patches only: by default, PatchManager only displays patches and updates. To view other software packages, deselect this option.

Per patch and client, several types of patching jobs can be planned. Right-click one or multiple patches and click **Check patches for usability** to run a job that checks if the selected patches apply to the selected clients. The **Software recognition** window pops up and allows you to schedule the job immediately or at a specific time, optionally repeated hourly, daily, weekly, or monthly. To install one or more patches, click **Install patches**. Like the Software recognition option, the **Software distribution** window lets you plan the distribution of patches. Patches can be installed immediately, after the next boot process, or after the next login. Optionally, you can delay patch installation. Click **Rollback** to plan a rollback job for patches that have already been deployed. To view more information and a description of any patch, click **Properties**.

The Status column will display the status of every patch and its planned or running patching jobs (e.g. *Scanning* while a job is being carried out, *Current* when the client already has the patch installed, or *Not applicable* when the patch does not apply).

Settings

The Settings panel controls several options related to patch deployment.



Settings

Status: ☑ Enabled

Client functions

☐ The user is allowed to view and request patches

☐ The user is allowed to refuse to have patches installed

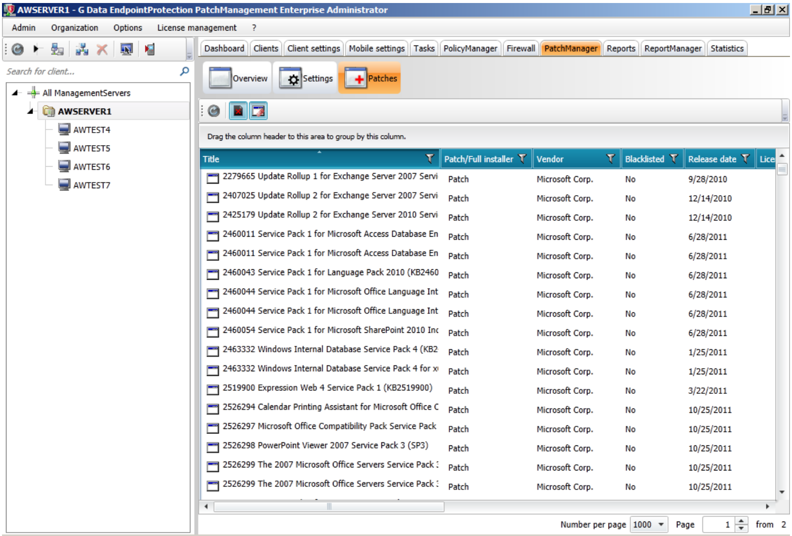
15 Minutes between installation attempts

3 Rollbacks prior to forced installation

Patch deployment can be enabled or disabled by ticking or unticking the **Enabled** checkbox. To allow a client to view available patches and file a request for deployment, tick **The user is allowed to view and request patches**. To allow a client to (temporarily) refuse patch installation, tick **The user is allowed to refuse to have patches installed**. You can select how many refusals are allowed until installation is forced, and how often patch installation should be attempted.

Patches

The Patches panel lists all available patches and lets you deploy them. While similar to the **Overview** panel, the Patches panel does not provide information on a per-client basis. Instead, it lists all available patches and lets you edit their priority.



Title	Patch/Full installer	Vendor	Blacklisted	Release date	Lice
2279665 Update Rollup 1 for Exchange Server 2007 Servi	Patch	Microsoft Corp.	No	9/28/2010	
2407025 Update Rollup 2 for Exchange Server 2007 Servi	Patch	Microsoft Corp.	No	12/14/2010	
2425179 Update Rollup 2 for Exchange Server 2010 Servi	Patch	Microsoft Corp.	No	12/14/2010	
2460011 Service Pack 1 for Microsoft Access Database En	Patch	Microsoft Corp.	No	6/28/2011	
2460011 Service Pack 1 for Microsoft Access Database En	Patch	Microsoft Corp.	No	6/28/2011	
2460043 Service Pack 1 for Language Pack 2010 (KB2460	Patch	Microsoft Corp.	No	6/28/2011	
2460044 Service Pack 1 for Microsoft Office Language Int	Patch	Microsoft Corp.	No	6/28/2011	
2460044 Service Pack 1 for Microsoft Office Language Int	Patch	Microsoft Corp.	No	6/28/2011	
2460054 Service Pack 1 for Microsoft SharePoint 2010 Inc	Patch	Microsoft Corp.	No	6/28/2011	
2463332 Windows Internal Database Service Pack 4 (KB2	Patch	Microsoft Corp.	No	1/25/2011	
2463332 Windows Internal Database Service Pack 4 for x	Patch	Microsoft Corp.	No	1/25/2011	
2519900 Expression Web 4 Service Pack 1 (KB2519900)	Patch	Microsoft Corp.	No	3/22/2011	
2526294 Calendar Printing Assistant for Microsoft Office C	Patch	Microsoft Corp.	No	10/25/2011	
2526297 Microsoft Office Compatibility Pack Service Pack	Patch	Microsoft Corp.	No	10/25/2011	
2526298 PowerPoint Viewer 2007 Service Pack 3 (SP3)	Patch	Microsoft Corp.	No	10/25/2011	
2526299 The 2007 Microsoft Office Servers Service Pack :	Patch	Microsoft Corp.	No	10/25/2011	
2526299 The 2007 Microsoft Office Servers Service Pack :	Patch	Microsoft Corp.	No	10/25/2011	

The list view is similar to that of the Overview panel. It lists all patches alphabetically, but does not display the status per client. To effectively manage the list, several filtering options are available:

Refresh: refresh the list to take the latest changes into account.

Hide patches on the blacklist: hide patches that have been added to the blacklist.

Display patches only: By default, PatchManager only displays patches and updates. To view other software packages, deselect Display patches only.

Right-click any one or multiple patches and click **Check patches for usability** to run a software recognition job, which checks if the selected patches apply to any of the managed clients. The **Software recognition** window pops up and allows you to schedule the job immediately or at a specific time, optionally repeated hourly, daily, weekly, or monthly. You can select one or more clients that should be checked for patch applicability.

To install one or more patches, Right-click any one or multiple patches and click **Install patches**. Like the Software recognition option, the **Software distribution** window lets you plan the distribution of patches. Patches can be installed immediately, after the next boot process, or after the next login. Optionally, you can delay patch installation.

To put one or more patches on the blacklist, right click it and select **Put patches on the blacklist** (this will update their status in the Blacklisted column to Yes). To remove a patch from the blacklist, right click it and select **Remove patches from the blacklist**. To view more information and a description of any patch, click **Properties**. The Properties window will show details about the patch, including the license, MD5 hash and URL for more information. Click **Show description** to view a detailed description of the patch.

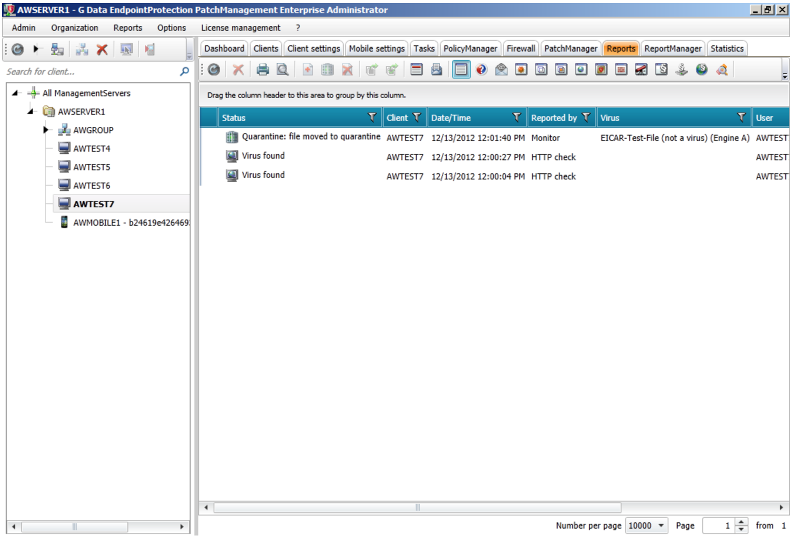
The Priority column will display the priority of every patch. The default priority is based on the PatchManager database, but can be edited (**Low**, **Normal**, or **High**).

Reports

All virus results, PolicyManager reports (if you are using G Data EndpointProtection), and firewall reports (with G Data ClientSecurity or EndpointProtection) are displayed in the Reports module, as well as system messages about installations, reboots, etc. The status 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. Infected files can be deleted or moved to the **Quarantine folder**. In the Reports module, 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.

Some reports allow you to directly plan a job. For example, if a client has requested a patch rollback, you can right click on the Rollback request report and select **Properties**. In the **Distribute software (rollback)** window you can then directly plan a rollback job, without having to open the **PatchManager** module to select the patch and client manually.



Status	Client	Date/Time	Reported by	Virus	User
Quarantine: file moved to quarantine	AWTEST7	12/13/2012 12:01:40 PM	Monitor	EICAR-Test-File (not a virus) (Engine A)	AWTEST
Virus found	AWTEST7	12/13/2012 12:00:27 PM	HTTP check		AWTEST
Virus found	AWTEST7	12/13/2012 12:00:04 PM	HTTP check		AWTEST

In the menu bar, an additional menu entry is available for the Reports module. For functions that operate with files (delete, move back, etc.), you must select one or more files in the list. You can select the following functions:

- **View**: Indicate whether you would like to see all reports, or only a subset of report types.

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

If you have set up scan jobs on your system, 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 file**: Attempt to remove the virus from the original file.
- **Move file to quarantine**: Move the selected files into the quarantine folder. The files will be encrypted and saved in the quarantine folder on the G Data ManagementServer, and the original files will be deleted. The encryption ensures that the virus cannot cause any damage. 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 to the **Security Labs service** for examination. 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**: Deletes the original file on the client.
- **Quarantine: clean & 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 client. If the virus cannot be removed, the file will not be moved back.
- **Quarantine: move back**: Moves the file from the quarantine folder back to the client. **Warning**: The file will be restored to its original state and will still be infected.
- **Quarantine: send in to G Data Security Labs**: If you discover a new virus or an unknown phenomenon, always send us the file. We will analyze the virus and send you a countermeasure as quickly as possible. Naturally our Security Labs will handle the data you sent with confidentiality and discretion.
- **Delete report**: 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 quarantined files are also deleted.

- **Delete dependent reports**: If a virus alert or a report is displayed twice or more due to tasks being performed multiple times, you can delete the duplicate entries from the log file using this option.

Toolbar actions

Refresh: Update the view and load the current reports from the G Data ManagementServer.

Delete: Deletes the selected report(s). If reports to which a quarantine file belongs are to be deleted, you must confirm the deletion once more. In this case, the quarantined files are also deleted.

Print: Print report(s). In the selection screen that appears, you can specify which details and areas you would like to print.

Page view: Preview the page to be printed

Remove virus

Move to quarantine

Delete file

Move file back from quarantine

Clean file & move back from quarantine

Hide dependent reports

Hide read reports

Display all reports

Display only errors and information

Display only email reports

Display only reports of unremoved viruses

Display only quarantine reports

Display only quarantine contents

Display only HTTP reports

Display only BankGuard reports

Display only firewall reports (in case you are using a software version with firewall)

Display only behavior blocker reports

Display only application control reports (in case you are using a software version with application control)

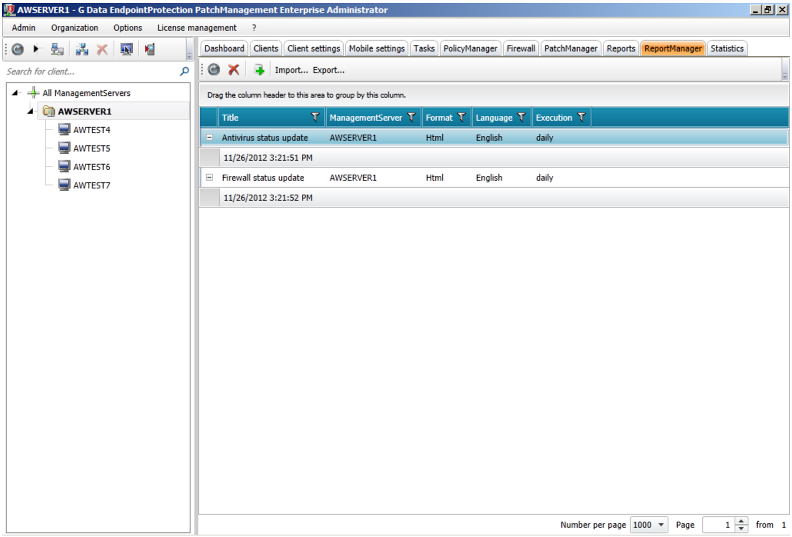
Display only device control reports (in case you are using a software version with device control)

Display only web control reports (in case you are using a software version with web content control)

Display only Update/Patch Management reports

ReportManager

ReportManager provides you with an overview of client statuses, protection and patch deployment. Reports can be generated regularly and distributed among predefined groups of recipients.



Title	ManagementServer	Format	Language	Execution
Antivirus status update	AWSERVER1	Html	English	daily
11/26/2012 3:21:51 PM				
Firewall status update	AWSERVER1	Html	English	daily
11/26/2012 3:21:52 PM				

Refresh: refresh the list.

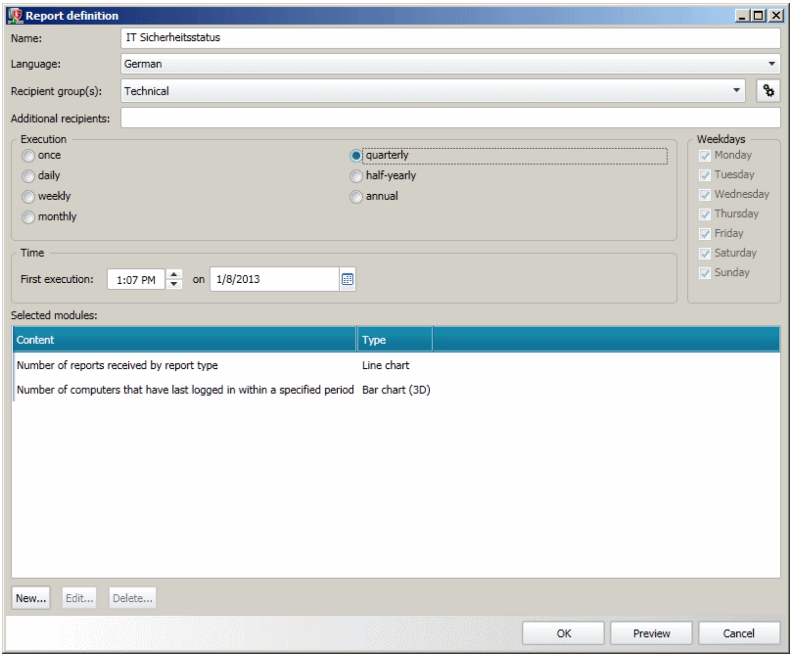
Delete: delete the selected report definition(s).

Add new report schedule: **define a new report** and schedule a reporting job.

To backup report definitions, click **Export...** to save them as a .dbdat file. Click **Import...** to restore definitions. Right-click one or more report definitions to **delete** them or click **execute immediately** to run the reporting job immediately. Click **Properties** to edit a report. **History** allows you to have a look at previously generated reports. If a reporting job has already been run, you can expand the report definition to see the associated reports and open them.

Report definition

The Report definition window allows you define a report containing one or more report modules, each of which covers a specific set of statistics and information. After selecting the appropriate modules, a reporting job can be scheduled to regularly generate the report.



Report definition

Name: IT Sicherheitsstatus

Language: German

Recipient group(s): Technical

Additional recipients:

Execution

○ once
○ daily
○ weekly
○ monthly
● quarterly
○ half-yearly
○ annual

Weekdays

☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday
☑ Sunday

Time

First execution: 1:07 PM on 1/8/2013

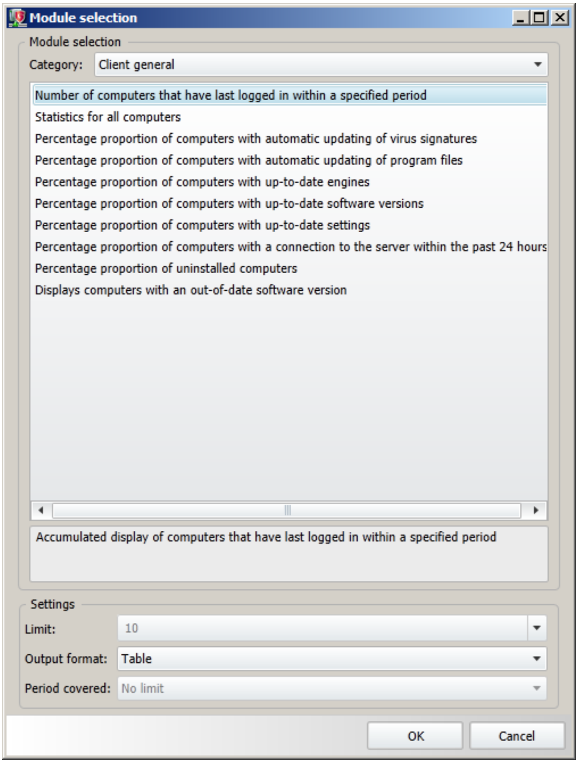
Selected modules:

Content	Type
Number of reports received by report type	Line chart
Number of computers that have last logged in within a specified period	Bar chart (3D)

The **Report definition** window features scheduling options that resemble the ones used for most other scheduled jobs. After defining a **name** and **language**, select the interval with which the report should be generated (once, daily, weekly, monthly, etc.). Under **Recipient group(s)**, you can add groups of e-mail recipients. Click the cogs icon to the right to define a new recipient group, if you haven't done so already in **Options** > **Server settings** > **Email settings**. You can also enter **additional recipients**, separated by commas.

Select module

To add a module to the report, click **New...** at the bottom of the screen to open the **Module selection** screen. Availability of the modules depends on the product version that you are using. The report modules have been divided into three categories: **Client general**, **client protection** and **PatchManager**. Select the appropriate module and define its settings at the bottom of the window. An output format can be selected for each module: **table**, **line chart**, **(3D) bar chart**, or **(3D) pie chart**. Not every module supports every output format. For some modules, you can also define a **limit** to the amount of items to be included, as well as a defined **period covered**. Click **OK** to add the selected module to the report. In the Module selection screen, click **Edit...** or **Delete...** to edit or delete modules. If you've finished selecting modules, click **Preview** to see a sample report, and **OK** to save the report definition.



Category: Client general

Number of computers that have last logged in within a specified period
Statistics for all computers
Percentage proportion of computers with automatic updating of virus signatures
Percentage proportion of computers with automatic updating of program files
Percentage proportion of computers with up-to-date engines
Percentage proportion of computers with up-to-date software versions
Percentage proportion of computers with up-to-date settings
Percentage proportion of computers with a connection to the server within the past 24 hours
Percentage proportion of uninstalled computers
Displays computers with an out-of-date software version

Accumulated display of computers that have last logged in within a specified period

Settings

Limit: 10

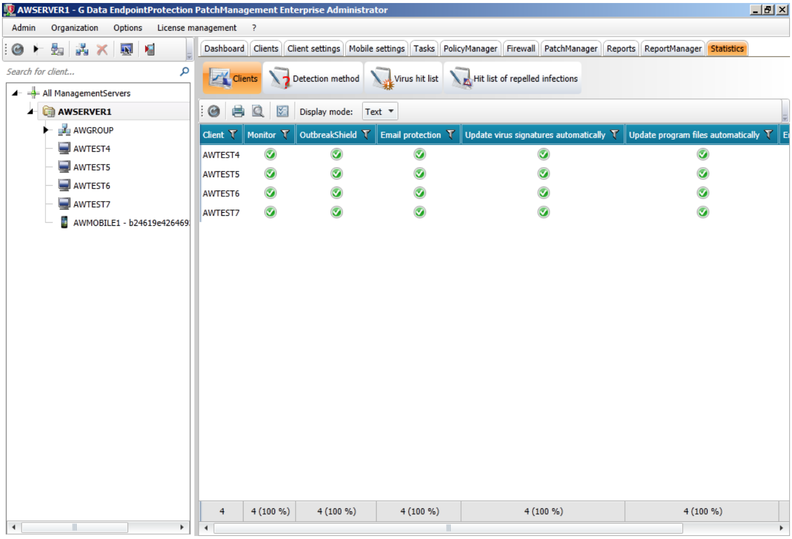
Output format: Table

Period covered: No limit

When a reporting job has been run, the resulting report will appear in the **ReportManager overview** and it will be sent to the defined recipients. Expand the report definition to see all instances. Double click on an instance to open the associated report.

Statistics

In the Statistics module, you can check statistical information about virus occurrences and client infections, as well as the security status of the managed network. Various views are available: the data can be displayed as text 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**, the **virus hit list** and the **hit list of repelled infections**. Select the relevant area in the display to view the data.



Display mode: Text

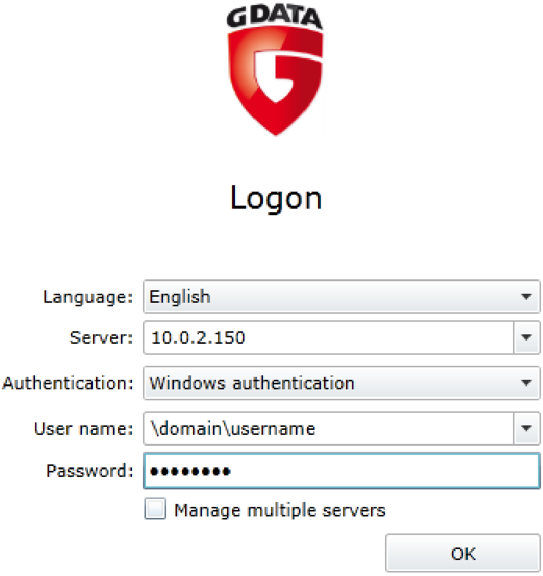
Client	Monitor	OutbreakShield	Email protection	Update virus signatures automatically	Update program files automatically	E
AWTEST4	✓	✓	✓	✓	✓	
AWTEST5	✓	✓	✓	✓	✓	
AWTEST6	✓	✓	✓	✓	✓	
AWTEST7	✓	✓	✓	✓	✓	
4	4 (100 %)	4 (100 %)	4 (100 %)	4 (100 %)	4 (100 %)	

G Data WebAdministrator

G Data WebAdministrator is the web-based control panel for G Data ManagementServer. It can be used to quickly edit and update settings through a web interface. In interface and function it is very similar to the central control panel G Data Administrator, but because it is browser-accessible, it can be accessed from virtually anywhere.

Starting G Data WebAdministrator

After completing the installation, G Data WebAdministrator can be started by double clicking the desktop icon. Alternatively, start your browser and navigate to the URL that has been provided at the end of the installation process. The URL consists of the IP address or computer name of the machine on which IIS is running and WebAdministrator has been installed, and the folder suffix (such as **http://10.0.2.150/GDAdmin/**). If you have not yet installed the Microsoft Silverlight browser plugin, you will be prompted to download it.



Logon

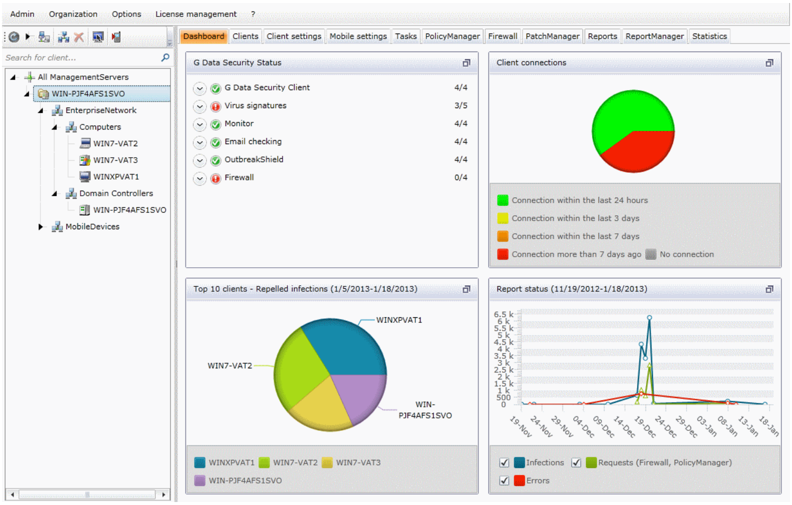
Language:	English
Server:	10.0.2.150
Authentication:	Windows authentication
User name:	\domain\username
Password:	•••••••••

□ Manage multiple servers

The WebAdministrator login page is very similar to the full **G Data Administrator** software. You will be prompted to enter **language**, **server**, **authentication**, **user name** and **password**. The server name should be filled in by default, but can be altered if necessary. Choose **Windows authentication** to log in with your Windows credentials, **SQL authentication** to log in with your SQL Server credentials, or **Integrated authentication** to use credentials that have been defined within the Administrator's **User account management**. Fill in your user name and password and click **OK** to log in.

Using G Data WebAdministrator

The interface of G Data WebAdministrator strongly resembles G Data Administrator. After a successful login, you will be presented with the central Dashboard, which provides an overview of the G Data ManagementServer(s) in your network and the associated clients.



G Data Security Status

G Data Security Client	4/4
Virus signatures	3/5
Monitor	4/4
Email checking	4/4
OutbreakShield	4/4
Firewall	0/4

🟩 Connection within the last 24 hours
🟨 Connection within the last 3 days
🟧 Connection within the last 7 days
🟥 Connection more than 7 days ago ⬜ No connection

Top 10 clients - Repelled infections (1/5/2013-1/18/2013)

WINXPVAT1 WIN7-VAT2 WIN7-VAT3
WIN-PJF4AFS1SVO

Report status (11/19/2012-1/18/2013)

☑ Infections ☑ Requests (Firewall, PolicyManager)
☑ Errors

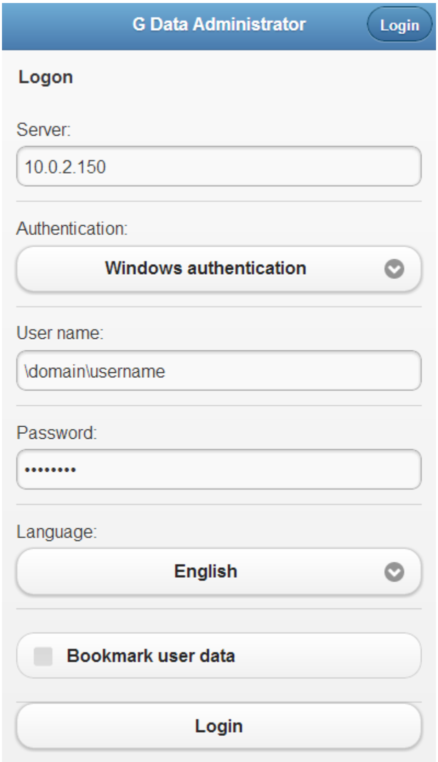
The functionality of WebAdministrator is identical to G Data Administrator. Please refer to the **appropriate chapter** for an in-depth overview.

G Data MobileAdministrator

G Data MobileAdministrator is the smartphone-accessible control panel for G Data ManagementServer. It can be used to quickly edit and update settings through an interface that has been optimised for mobile devices. The most important and frequently used options are presented in a responsive design that adapts to various mobile environments.

Starting G Data MobileAdministrator

After completing the installation, G Data MobileAdministrator can be started from any browser. Start your browser and navigate to the URL that has been provided at the end of the installation process. The URL consists of the IP address or computer name of the machine on which IIS is running and WebAdministrator has been installed, and the folder suffix (such as **http://10.0.2.150/GDMobileAdmin/**).



Server: 10.0.2.150

Authentication: Windows authentication

User name: \domain\username

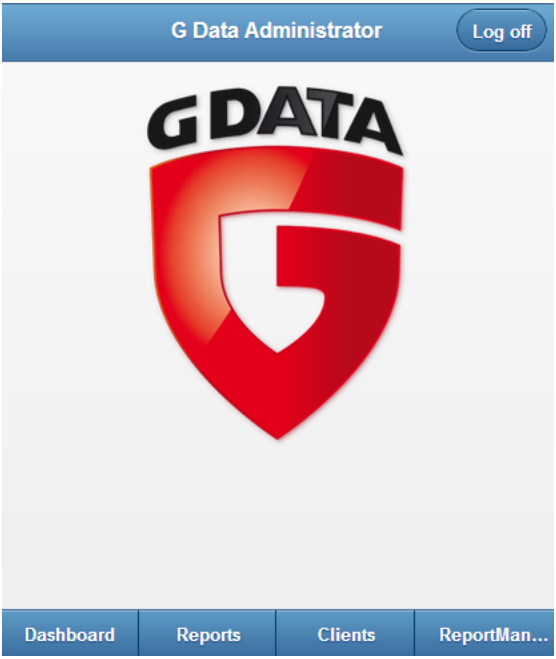
Password: ••••••••

Language: English

The MobileAdministrator login page supports the same login methods as **G Data Administrator** and **WebAdministrator**. You will be prompted to enter **language**, **server**, **authentication**, **user name** and **password**. Choose **Windows authentication** to log in with your domain credentials, **SQL authentication** to log in with your SQL Server credentials, or **Integrated authentication** to use credentials that have been defined within the Administrator's **User account management**. If you want your credentials and language settings to be remembered next time, tick the checkbox **Bookmark user data.** Tap **Login** to log in.

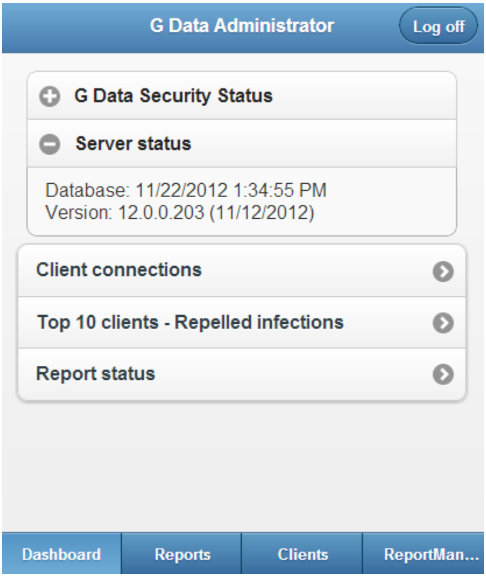
Using G Data MobileAdministrator

After logging in to G Data MobileAdministrator the main menu is displayed. Four branches of options are available: **Dashboard**, **Reports**, **Clients**, and **ReportManager**. To log off, tap **Log off** in the top right corner of the screen.



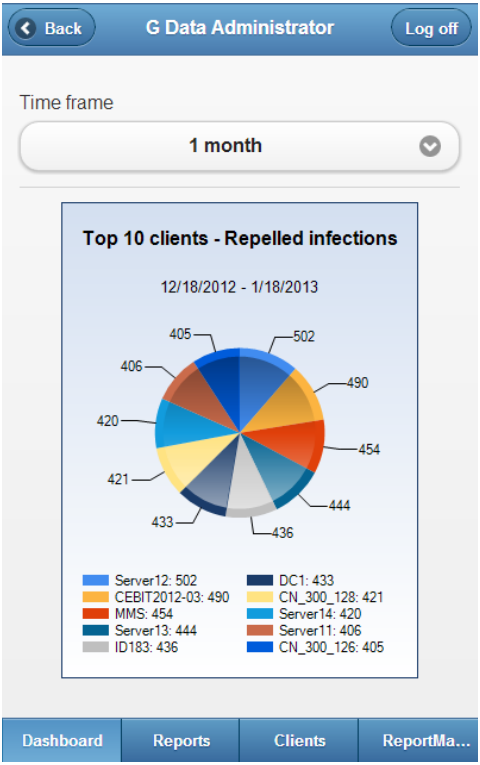
Dashboard

The Dashboard of G Data MobileAdministrator allows you to view the most important statistics at a glance. Comparable to the Dashboard of G Data Administrator, it provides an overview of the status of G Data ManagementServer and its clients. Additionally, you can view statistics about client connections and repelled infections.



Database: 11/22/2012 1:34:55 PM
Version: 12.0.0.203 (11/12/2012)

Select **G Data Security Status** to view extensive information about the status of server and clients. MobileAdministrator will show you how many machines have the G Data Security Client installed, as well as information about (outdated) virus signatures and program components such as monitor, email checking, OutbreakShield and firewall. Engine rollbacks can be managed by opening the virus signatures subsection. The status of ManagementServer itself can be viewed by expanding **Server status**.



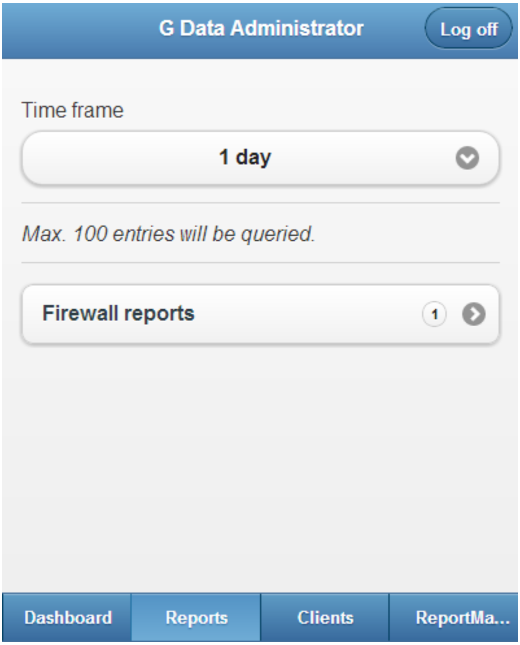
Time frame

1 month

Statistics are available under **Client connections** and **Top 10 clients - Repelled infections**. Tap **Report status** to check on infection, request and error reports.

Reports

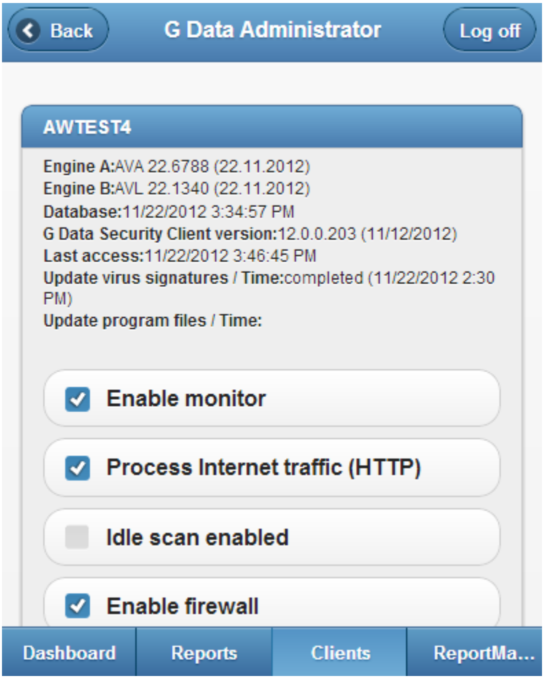
The Reports view presents virus, firewall and PolicyManager reports. It is a mobile-optimized representation of the same information that is available in the **Reports** module of G Data Administrator.



Select the period (**Time frame**) for which you want to view reports (1 day, 7 days or 1 month). MobileAdministrator will return the different categories for which reports are available. Tap a category to view the individual reports available. Reports can be filtered by name. Any report can be opened to check on further details and take action, if necessary.

Clients

MobileAdministrator offers a concise overview of all clients that are managed by G Data ManagementServer. Per client, in-depth information is available and several security settings can be edited.



AWTEST4

Engine A:AVA 22.6788 (22.11.2012)
Engine B:AVL 22.1340 (22.11.2012)
Database:11/22/2012 3:34:57 PM
G Data Security Client version:12.0.0.203 (11/12/2012)
Last access:11/22/2012 3:46:45 PM
Update virus signatures / Time:completed (11/22/2012 2:30 PM)
Update program files / Time:

☑ Enable monitor

☑ Process Internet traffic (HTTP)

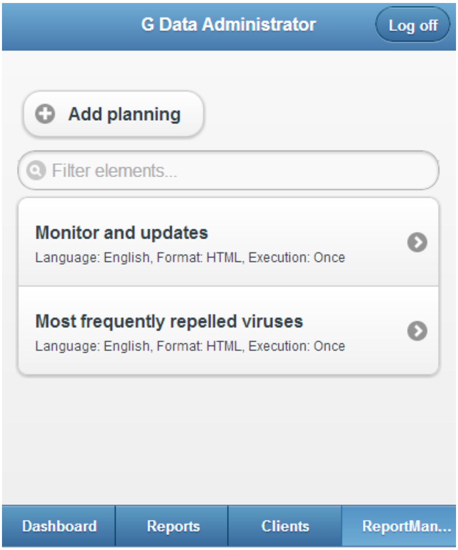
☐ Idle scan enabled

☑ Enable firewall

The Clients overview provides a list of all machines that are being managed by G Data ManagementServer. The list can be filtered by name. By selecting an individual machine, you can check several statistics about versions and updates. Additionally, several security settings can be edited. Enable or disable **monitor**, **HTTP traffic processing**, **idle scan** or **firewall** by ticking or unticking the appropriate checkboxes. Policy settings such as **Application control**, **Device control**, **Web content control**, and **Internet usage time** can also be controlled from this view. Tap **Save** to save the machine's settings.

ReportManager

ReportManager is the mobile version of the **ReportManager** module in G Data Administrator. It allows you to configure, schedule and preview reporting jobs.



Monitor and updates
Language: English, Format: HTML, Execution: Once

Most frequently repelled viruses
Language: English, Format: HTML, Execution: Once

To add a new job, tap **Add planning**. Existing reporting jobs are listed in the main view of ReportManager and can be edited by tapping them. The job view lets you edit all aspects of the job. Enter a **name**, define the **language** and select a **recipient group** or enter **additional recipient(s)**. The job can be scheduled by selecting an **interval** and defining **time** and **date**. Under **Selected modules**, you can choose the reporting modules to be included in the report. These are identical to the modules that are available through G Data Administrator. Edit, add or delete modules and tap **Save** to return to the job view. If necessary, **preview** the report, then **save** it. Redundant or unnecessary jobs can be deleted.

G Data Security Client

The client software provides virus protection and runs the G Data ManagementServer jobs allocated to it in the background. The clients have their own virus signatures and scheduler, so that virus analysis can also be run in offline mode (e.g. for notebooks that do not have a continuous connection to the G Data ManagementServer).

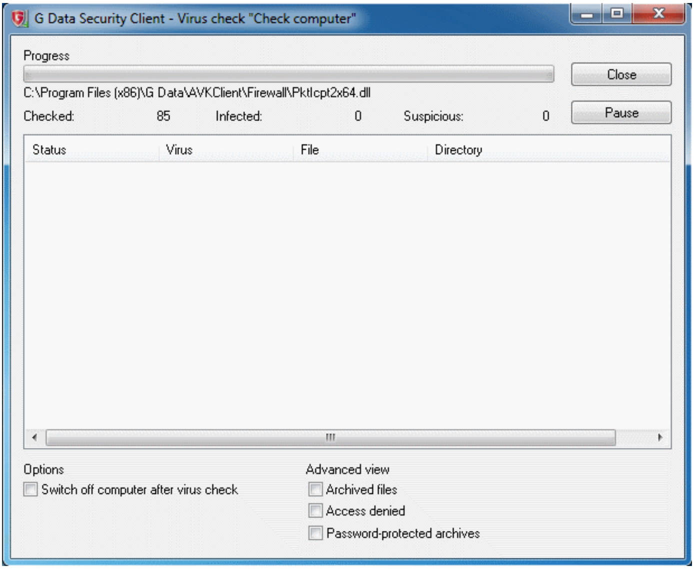
System tray

After the installation of the client software, a system tray icon is available to the user of the client to carry out tasks independently of administrative schedules. Which options are available needs to be approved and defined using the **Client settings** module of G Data Administrator.

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

Virus check

With this option, a user can carry out a targeted virus check on the computer using G Data Security Client, even outside of the virus checking schedule specified in G Data Administrator.



G Data Security Client - Virus check "Check computer"

Progress

C:\Program Files (x86)\G Data\AVKClient\Firewall\Pktlcpt2x64.dll

Checked: 85 Infected: 0 Suspicious: 0

Options

□ Switch off computer after virus check

Advanced view

□ Archived files

□ Access denied

□ Password-protected archives

The user can check removable devices, CDs/DVDs, memory, the 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. Clients can use the **Options** window to configure actions that should be taken when a virus is found, such as moving virus-infected files to a local quarantine folder.

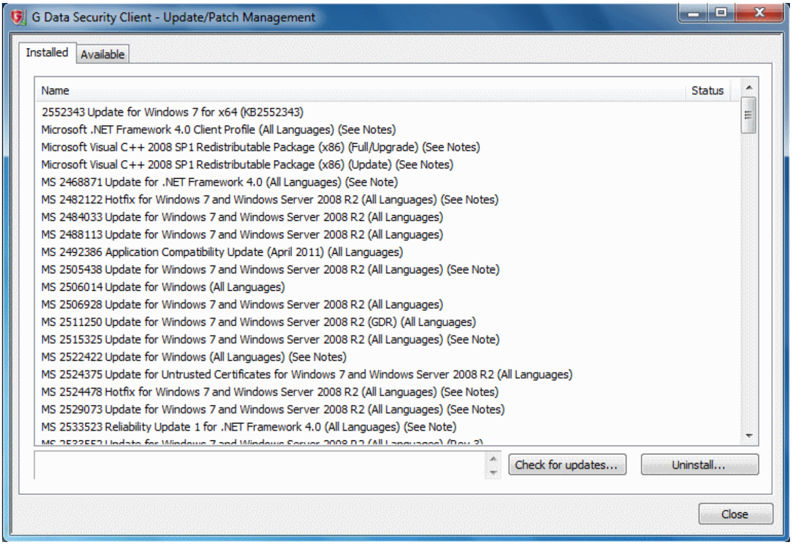
> The user can also easily check files or directories from Windows Explorer by selecting the files or directories and using the **Check for viruses (G Data AntiVirus)** option in the context menu.

While a virus scan is running, whether it has been initiated locally or is part of a scan job, the context menu is expanded with the following entries:

- **Virus check priority**: Set the priority of the virus check. With **High**, the virus check is carried out quickly, but it can significantly slow down other programs on the computer. With the **Low** setting, on the other hand, the virus check takes a comparatively long time, but other applications on the client computer are not significantly slowed down (only available for local scan jobs).
- **Pause virus check**: Pause a locally started virus check. Scan jobs that are have been initiated by G Data ManagementServer can only be stopped if the administrator has enabled the **User can halt or cancel the scan job** option when setting up the job.
- **Cancel virus check**: Cancel a locally started virus check. Scan jobs that are have been initiated by G Data ManagementServer can only be cancelled if the administrator has enabled the **User can halt or cancel the scan job** option when setting up the job.
- **Display scan window**: Display the progress and results of the virus check (only available for local scan jobs).

Updates/Patches

If the administrator chooses to enable the option **The user is allowed to view and request patches** in G Data Administrator's **PatchManager** module, the Security Client will offer an Updates/ Patches option in its system tray menu. Clicking on it reveals a patch/update overview for the client pc, divided over two tabs.



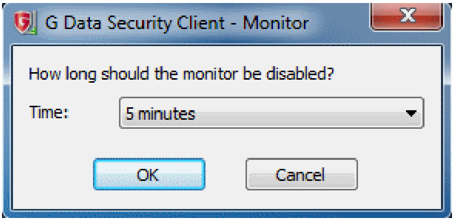
Name	Status
2552343 Update for Windows 7 for x64 (KB2552343)	
Microsoft .NET Framework 4.0 Client Profile (All Languages) (See Notes)	
Microsoft Visual C++ 2008 SP1 Redistributable Package (x86) (Full/Upgrade) (See Notes)	
Microsoft Visual C++ 2008 SP1 Redistributable Package (x86) (Update) (See Notes)	
MS 2468871 Update for .NET Framework 4.0 (All Languages) (See Note)	
MS 2482122 Hotfix for Windows 7 and Windows Server 2008 R2 (All Languages) (See Notes)	
MS 2484033 Update for Windows 7 and Windows Server 2008 R2 (All Languages)	
MS 2488113 Update for Windows 7 and Windows Server 2008 R2 (All Languages)	
MS 2492386 Application Compatibility Update (April 2011) (All Languages)	
MS 2505438 Update for Windows 7 and Windows Server 2008 R2 (All Languages) (See Note)	
MS 2506014 Update for Windows (All Languages)	
MS 2506928 Update for Windows 7 and Windows Server 2008 R2 (All Languages)	
MS 2511250 Update for Windows 7 and Windows Server 2008 R2 (GDR) (All Languages)	
MS 2515325 Update for Windows 7 and Windows Server 2008 R2 (All Languages) (See Note)	
MS 2522422 Update for Windows (All Languages) (See Notes)	
MS 2524375 Update for Untrusted Certificates for Windows 7 and Windows Server 2008 R2 (All Languages)	
MS 2524478 Hotfix for Windows 7 and Windows Server 2008 R2 (All Languages) (See Notes)	
MS 2529073 Update for Windows 7 and Windows Server 2008 R2 (All Languages) (See Notes)	
MS 2533523 Reliability Update 1 for .NET Framework 4.0 (All Languages) (See Note)	
MS 2533552 Update for Windows 7 and Windows Server 2008 R2 (All Languages) (Rev 3)	

The **Installed** tab shows all patches and updates that have been installed on the system. Double click a patch to view an extended description. If a patch or update seems to be causing problems, users can select it and click **Uninstall** to ask the administrator to remove it. The **Status** will change to **Waiting for response** and the administrator will receive a **report** with a rollback request. To perform a local check, regardless of software recognition jobs planned on the ManagementServer, click **Check for updates**. Security Client will then check all patches for applicability on the local system.

The **Available** tab list patches, updates and software packages that are applicable to the client system. Double click an item to view an extended description. To request installation, click **Install**. The **Status** will change to **Waiting for response** and the administrator will receive a **report** with a software distribution request.

Disable monitor

Using the Disable monitor command, the user can switch off G Data Monitor for a specified time (from 5 minutes up to until the next computer restart). This is only possible if the system administrator has enabled the option. Switching off the monitor temporarily may be useful during extensive file copying procedures, as this would considerably speed the process up. However, extra care should be taken as real-time virus checking is switched off during this interval.



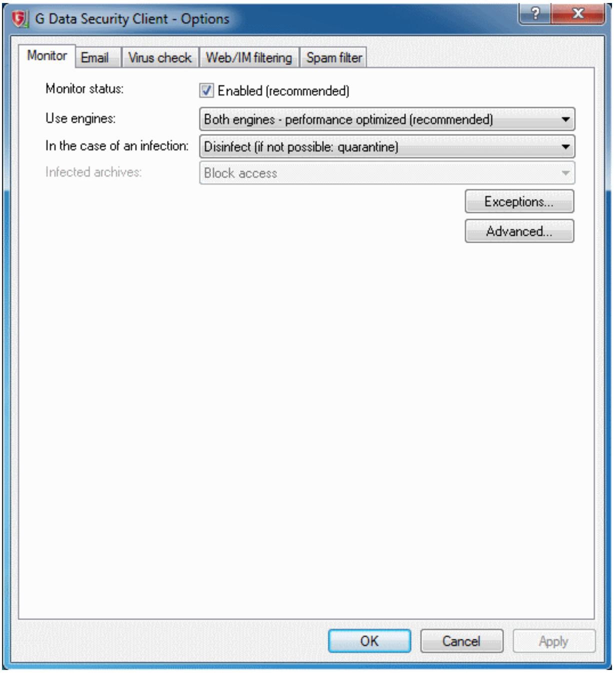
G Data Security Client - Monitor

How long should the monitor be disabled?

Time: 5 minutes

Options

If the system administrator has enabled the option **The user can change email and monitor options** in the **Client settings module**, the user can adjust security options on the **Monitor**, **Email**, **Web/IM filtering** and **Spam filter** tabs. In this way, all client protection mechanisms of the G Data software can be disabled. This option should therefore only be accessible to technically experienced users. The settings on these tabs are explained in detail in the chapter **Client settings**.



Monitor status: ☑ Enabled (recommended)

Use engines: Both engines - performance optimized (recommended)

In the case of an infection: Disinfect (if not possible: quarantine)

Infected archives: Block access

If you enable the option **The user can run virus checks**, users can check their client computer for viruses independently of the scan jobs scheduled on the G Data ManagementServer. A virus check can be initiated by clicking **Virus check** in the system tray context menu. The settings on the **Virus check** tab correspond to those found on the **Monitor** tab in the **Client settings** module.

The security-relevant settings under Options can also be password-protected. The administrator assigns the client an individual password, with which the user can change security options. This password is granted in the Client Settings module under **Protect options with a password**.

Quarantine

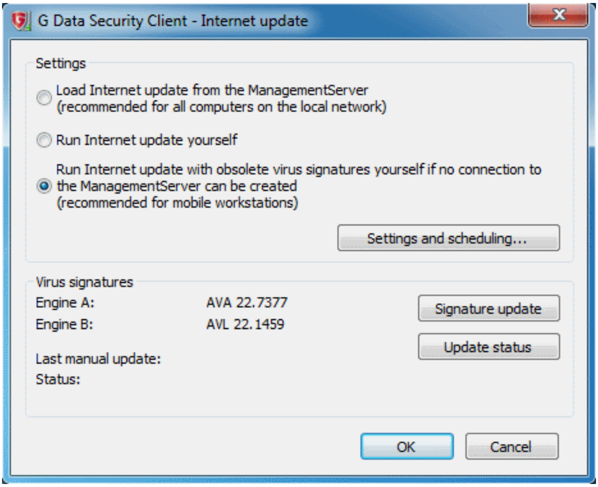
Every client has a local quarantine folder into which infected files (depending on the settings for the monitor/scan job) can be moved. A file that has been moved into quarantine cannot execute any malware. Infected files are automatically zipped and encrypted when they are moved to quarantine. When quarantining 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 G Data ManagementServer. These settings cannot be changed. The client quarantine is located in the directory *%ProgramData%\G DATA\AntiVirusKit Client\Quarantine*. The G Data ManagementServer quarantine is located in the directory *%ProgramData%\G DATA\AntiVirus ManagementServer\Quarantine*.

If an infected file of less than 1 MB is detected on a client without a connection to G Data ManagementServer, it is saved in the local quarantine and only transferred to the central quarantine upon the next contact with G Data 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 a file does not remove the virus. You should only select this option if a program cannot run without the infected file and you nevertheless need it for data recovery.

Internet update

G Data Security Client can also be used to carry out virus signature updates from the Internet if no connection to G Data ManagementServer is available. This option can be enabled for individual clients by the network administrator. Use the **Settings and scheduling** button to schedule virus updates locally.



G Data Security Client - Internet update

Settings

○ Load Internet update from the ManagementServer (recommended for all computers on the local network)

○ Run Internet update yourself

● Run Internet update with obsolete virus signatures yourself if no connection to the ManagementServer can be created (recommended for mobile workstations)

Virus signatures

Engine A: AVA 22.7377

Engine B: AVL 22.1459

Last manual update:

Status:

Firewall

The Firewall module is only available as part of the ClientSecurity (Enterprise/Business) and EndpointProtection (Enterprise/Business) **solutions**.

Users can make extensive changes to their firewall settings, if this option has been switched on by the administrator. As long as the client is in the G Data ManagementServer network, the firewall will 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 MailSecurity MailGateway

G Data MailSecurity provides complete protection of your corporate email communication. It comprises:

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

Configuring G Data MailSecurity MailGateway

In addition to the actual software, which runs in the background, the installation wizard also installs **G Data MailSecurity Administrator**, which gives you full access to the functions and options of MailGateway. MailSecurity Administrator can be found under **Start** > **Programs** > **G Data MailSecurity** > **G Data MailSecurity**. If you close the administrator software, MailGateway will remain active in the background.

You can also maintain MailGateway using any other computer, as long as it meets the system requirements for MailSecurity Administrator. To install MailSecurity Administrator on another PC without installing the full MailGateway, simply start the setup and choose the **G Data MailSecurity Administrator** button.

Protocols

Sending and receiving email is generally based on the SMTP and POP3 protocols. SMTP is used to send email to any recipient whereas POP3 is used to store received email in a mailbox, which can only be accessed by the recipient by means of a password. Depending on how your network is set up, G Data MailSecurity can use various nodes to check incoming email for virus infections:

- If you are using an SMTP server in your network, G Data MailSecurity can check incoming email even before it reaches the mail server. This can be set up using the **Check incoming email (SMTP)** function in the **Status module**.
- If you receive your email directly from an external POP3 server (e.g., via a POP3 collective account), G Data MailSecurity can

also be implemented to check the POP3 email for viruses before opening by the recipient. This can be set up using the **Scanning incoming email (POP3)** function in the **Status module**.

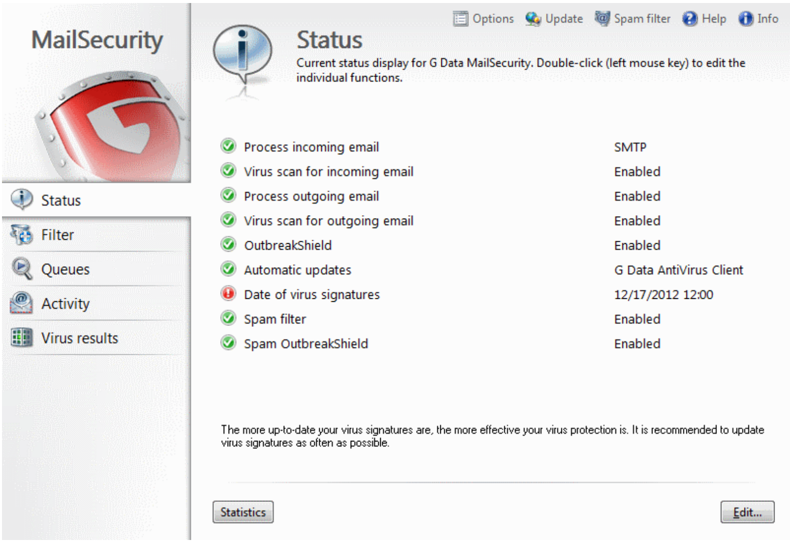
G Data MailSecurity can also scan all your outgoing email for virus infections before sending anything to the recipient. Since only the SMTP protocol is used for sending email, there is no POP3 variant for this. This can be set up using the **Scanning outgoing email (SMTP)** function in the **Status module**.

Exchange support

G Data MailSecurity can optionally be installed as a plugin for Microsoft Exchange Server 2007/2010 to provide proactive on-demand and on-access protection for all emails that are sent and received through Microsoft Exchange Server.

G Data MailSecurity Administrator

G Data MailSecurity Administrator is the administration software for G Data MailSecurity MailGateway, which protects all SMTP- and POP3-based email traffic within your entire network. Administrator can be started from any computer running Windows, using password protection. Remote configuration is possible for all virus protection and signature update settings.



Status

Current status display for G Data MailSecurity. Double-click (left mouse key) to edit the individual functions.

✓ Process incoming email	SMTP
✓ Virus scan for incoming email	Enabled
✓ Process outgoing email	Enabled
✓ Virus scan for outgoing email	Enabled
✓ OutbreakShield	Enabled
✓ Automatic updates	G Data AntiVirus Client
! Date of virus signatures	12/17/2012 12:00
✓ Spam filter	Enabled
✓ Spam OutbreakShield	Enabled

The more up-to-date your virus signatures are, the more effective your virus protection is. It is recommended to update virus signatures as often as possible.

Starting G Data MailSecurity Administrator

You can use Administrator to control the mail gateway by clicking on the entry **G Data MailSecurity Administrator** in the program group **Start** > **(All) Programs** > **G Data MailSecurity**.

When you start Administrator for the first time, you will be asked for the server and password. In the **Server** field, enter the computer name or the IP address of the computer on which MailGateway has been installed. Since no **password** has been assigned yet, simply click the **OK** button without entering a password. A password entry window now opens in which you can enter a **new password**. Confirm the password by typing it again and click **OK**. On the **Advanced** tab of the **Options** menu, you can change the password at any time by clicking the **Change password** button.

Subsequent starts

You can use the Administrator tool to control the mail gateway by clicking on the entry **G Data MailSecurity Administrator** in the program group **Start** > **(All) Programs** > **G Data MailSecurity** in the start menu. When you start Administrator, you will be asked for the server and password. In the **Server** field, enter the computer name or the IP address of the computer on which the MailGateway has been installed.

Configuring G Data MailSecurity Administrator

The menu bar at the top of G Data MailSecurity Administrator offers you the following options for configuration:

Options: Change the basic settings for operating G Data MailSecurity.

Update: Configure automatic virus signatures updates. Schedule signature downloads and update the G Data MailSecurity program files.

Spam filter: Effectively block email with undesirable content or from undesirable senders (e.g. mass email senders).

Help: Access the online help for the product.

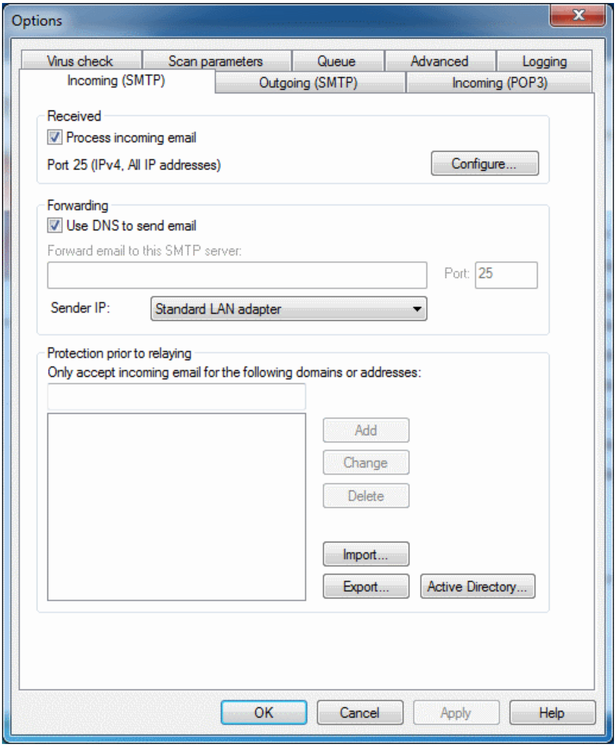
Info: Information about the program version.

Options

The Options window allows you to configure a vast range of settings, in order to adapt G Data MailSecurity optimally to the conditions in your network.

Incoming (SMTP)

On the Incoming (SMTP) tab you can configure the virus scan for incoming SMTP email on your mail server.



Received

☑ Process incoming email

Port 25 (IPv4, All IP addresses)

Forwarding

☑ Use DNS to send email

Forward email to this SMTP server:

Port: 25

Sender IP: Standard LAN adapter

Protection prior to relaying

Only accept incoming email for the following domains or addresses:

Received

Under Received you can specify whether Incoming email should be processed. This is generally done over port 25. If this standard port should not be used under particular circumstances, you can define other port and protocol settings for incoming email using the button **Configure**.

Forwarding

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

Protection prior to relaying

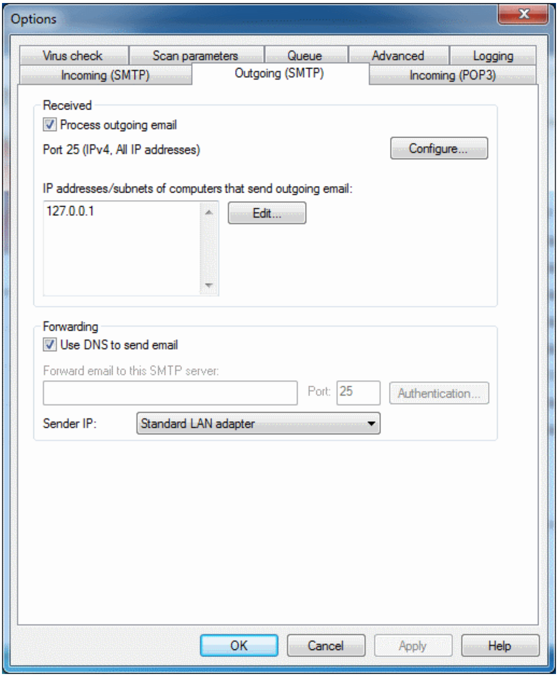
To prevent your mail server from being abused, you should specify the domains to which SMTP email may be sent under **Only accept incoming email from the following domains**. This way, your server cannot be misused for forwarding spam to other domains.

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

If you want, you can also implement relay protection using a list of valid email addresses. Email messages to recipients that are not on the list are not accepted. To automate the maintenance of these email addresses, these can be read automatically and periodically from **Active Directory**. The Active Directory connection requires at least .NET Framework 1.1.

Outgoing (SMTP)

On the Outgoing (SMTP) tab you can configure the scanning of outgoing SMTP email on your mail server.



Received

☑ Process outgoing email

Port 25 (IPv4, All IP addresses)

IP addresses/subnets of computers that send outgoing email:

127.0.0.1

Forwarding

☑ Use DNS to send email

Forward email to this SMTP server:

Port: 25

Sender IP: Standard LAN adapter

Received

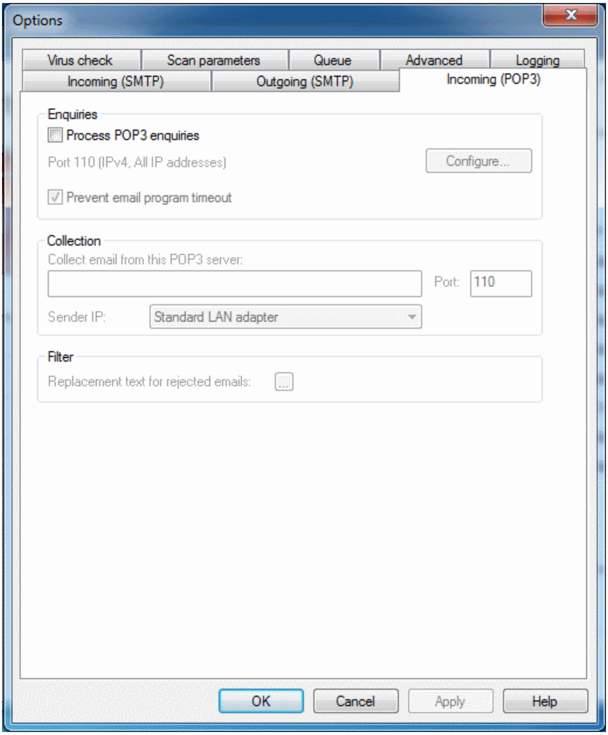
Check **Process outgoing email** to enable checking outgoing SMTP email for viruses. Under **IP addresses/subnets for computers that send outgoing email** you can specify from which IP addresses the email to be checked originates. If there are several possible IP addresses, use a comma to separate them. This input is required so that the email gateway can distinguish between incoming and outgoing email. In general, port 25 is configured to accept outgoing emails. If this standard port should not be used under particular circumstances, you can define port and protocol settings for incoming email via the button **Configure**.

Forwarding

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

Incoming (POP3)

On the Incoming (POP3) tab, you can configure virus scans for incoming POP3 email on your mail server.



Enquiries

☐ Process POP3 enquiries

Port 110 (IPv4, All IP addresses)

☑ Prevent email program timeout

Collection

Collect email from this POP3 server:

Port: 110

Sender IP: Standard LAN adapter

Filter

Replacement text for rejected emails:

Enquiries

Use **Process POP3 enquiries** to let G Data MailSecurity fetch your POP3 emails from a POP3 server, check them for viruses and forward them to their recipients via your email server. Where applicable, you must specify the **port** that your email program uses for POP3 enquiries (normally port 110). Depending on the amount of email, there can be a delay of several seconds when the user retrieves POP3 emails. Tick **Prevent email program timeout** to prevent the recipient from getting a timeout error from their email software if POP3 retrieval is taking too long.

POP3-based email programs can be configured manually. Use 127.0.0.1 or your email gateway server as the inbound POP3 server in your email program and separate the name of the external email server from your user name with a colon. For example, instead of *POP3 server:mail.xxx.net/user name:Jane Q. Public*, you write *POP3 server:127.0.0.1/user name:mail.xxx.com:Jane Q. Public*. To perform a manual configuration, please refer to the manual of your email program.

Collection

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

Filter

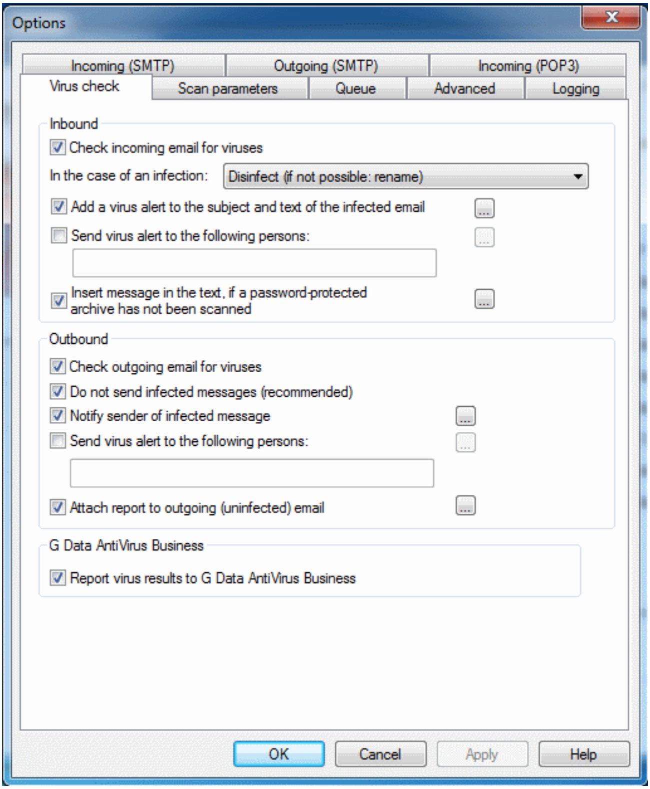
If POP3 email is rejected based on a content check or due to a virus infection, the message sender can be automatically informed. The default message for rejected email is: *The message was rejected by the system administrator*. However, the notification can be changed. You can use wildcards to copy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

- %v > Virus
- %s > Sender
- %r > Recipient
- %c > Cc

- %d > Date
- %u > Subject
- %h > Header
- %i > Sender IP

Virus check

The Virus check tab lets you set virus check options for incoming and outgoing email.



Options

Inbound

☑ Check incoming email for viruses

In the case of an infection: Disinfect (if not possible: rename)

☑ Add a virus alert to the subject and text of the infected email

□ Send virus alert to the following persons:

☑ Insert message in the text, if a password-protected archive has not been scanned

Outbound

☑ Check outgoing email for viruses

☑ Do not send infected messages (recommended)

☑ Notify sender of infected message

□ Send virus alert to the following persons:

☑ Attach report to outgoing (uninfected) email

G Data AntiVirus Business

☑ Report virus results to G Data AntiVirus Business

Inbound

In almost all cases, you should enable **Check incoming email for viruses** and also check which option you want to use **in case of an infection**.

- **Log only**
- **Disinfect (if not possible: log only)**
- **Disinfect (if not possible: rename)**
- **Disinfect (if not possible: delete)**
- **Rename infected attachments**
- **Delete infected attachments**
- **Delete message**

Options in which incoming viruses are only logged, should only be used if your system is permanently protected from viruses another way (e.g., using the client/server-based virus protection G Data AntiVirus).

If a virus is found you have a wide range of notification options. You can add a virus alert to the subject and text of the infected email in order to inform the recipient. You can also send a virus discovery alert to inform certain persons (e.g. system administrators) that a virus has been sent to an email address in your network. Separate multiple recipient addresses with a semicolon.

You can customize the text for the notification functions. Wildcards can be used here to add information to the notification text. In the **Subject** and **Email text** fields, the following wildcards (defined using a percentage symbol followed by a lower case letter) are available:

- %v > Virus
- %s > Sender
- %r > Recipient
- %c > Cc
- %d > Date
- %u > Subject

- %h > Header
- %i > Sender IP

Outbound

In general, you should enable **Check outgoing email for viruses** and also have **Do not send infected messages** activated by default. This way, viruses cannot leave your network and won't cause any damage to your business partners. If a virus is found you have a wide range of notification options. You can choose **Notify sender of infected message**, and under **Send virus alert to the following persons** notify a system administrator or responsible employee of the fact that a virus was about to be sent from your network. Please separate multiple recipient addresses with a semicolon.

You can customize the notification texts. To do this, simply click the **...** button to the right. Wildcards can be used here to add information to the notification text. In the **Subject** and **Email text** fields, the following wildcards (defined using a percentage symbol followed by a lower case letter) are available:

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

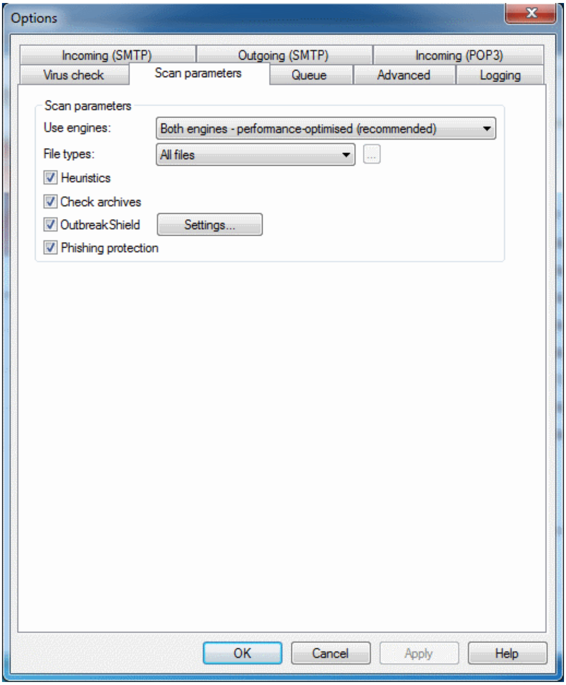
In addition, under **Attach report to outgoing (uninfected) email**, you have the option of sending email checked by G Data MailSecurity with a note at the end of the email text pointing out explicitly that this mail has been checked by G Data MailSecurity. You can customise this report or leave it out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

G Data AntiVirus Business

If MailGateway is being operated as part of a G Data business solution, you can enable **Report virus results to G Data AntiVirus Business** to make sure that the G Data AntiVirus client/server-based antivirus software is informed of MailGateway virus discoveries so that it can provide you with a comprehensive overview of virus infections in your network.

Scan parameters

On this tab, you can optimize the virus detection performance of G Data MailSecurity and configure it to your individual requirements. In general, reducing the virus detection increases the overall performance of the system, while increasing it might result in slight performance losses.



Scan parameters

Use engines: Both engines - performance-optimised (recommended)

File types: All files

☑ Heuristics

☑ Check archives

☑ OutbreakShield Settings...

☑ Phishing protection

The following functions are available:

- **Use engines**: The G Data software works with two independently operating virus scanning engines. Using both engines guarantees optimum results for preventing viruses. Using just one engine may have performance advantages.
- **File types**: Under **File types**, you can define the file types G Data MailSecurity should check for viruses. G Data recommends automatic type recognition, which checks only those files that might theoretically contain a virus. If you want to define the file types to be checked for viruses yourself, use the **user-defined** function. By clicking the **...** button you can open a dialogue box in which you enter the file types you want into the upper input field and then use the **Add** button to add them to the list of user-defined file types. You can also use wildcards, i.e. replace characters or strings of characters.

  > The question mark symbol (?) represents individual characters. The asterisk symbol (*) represents entire character strings. For instance, in order to check all files with the file extension **.exe**, enter ***.exe**. For example, to check files with different spreadsheet formats (e.g., **.xlr**, **.xls**), simply enter ***.xl?**. For instance, to check files of various types that have identical initial file names, enter **text*.*** for example.

- **Heuristics**: In a heuristic analysis viruses are not only detected using the constantly updated virus signature databases but also by identifying certain features characteristic of viruses. This method is an additional security benefit, but in rare cases it may lead to false alarms.
- **Check archives**: Checking of compressed files in archives should generally be activated.
- **OutbreakShield**: OutbreakShield detects and neutralizes threats from malicious programs in mass emails before the relevant up-to-date virus signatures become available. OutbreakShield uses the Internet to monitor increased volumes of suspicious email, enabling it to close the window between the mass email outbreak and its containment with specially adapted signatures, practically in real time. If you want to use OutbreakShield, use the **Settings** button to specify whether you are using a proxy server and, if necessary, the **Access**

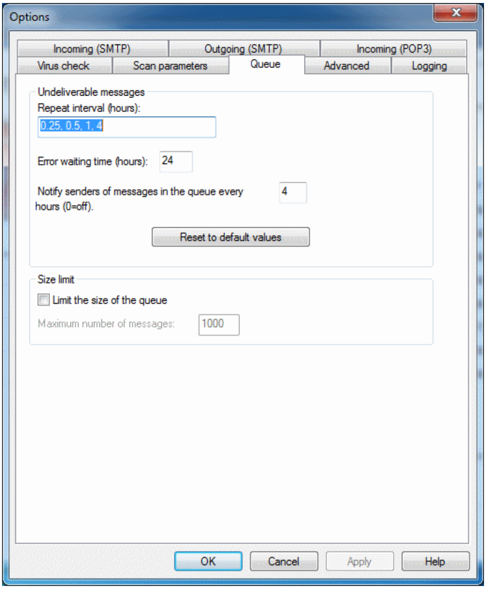
data for Internet connection to enable OutbreakShield to access the Internet at any time. On the OutbreakShield tab, you can define the text of the email that a mail recipient receives if a mass email addressed to him/her has been rejected.

> Due to its independent architecture, OutbreakShield cannot disinfect, rename or quarantine infected email attachments. Hence, the replacement text informs the user that a suspicious or infected email was not delivered. If you have selected **Delete message** as action on the **Virus check** tab, OutbreakShield will not send a notification for rejected email. In this case, all infected emails, including those that have been only detected by OutbreakShield, are deleted directly.

Queue

On the Queue tab, you can specify how often and at what intervals email that cannot be forwarded from MailGateway to the mail server should be resent.

In general, email only reaches the queue after a virus check by G Data MailSecurity. Email can be in the queue for a number of reasons. For example, the mail server to which they are to be forwarded may be overloaded or may have failed.



Undeliverable messages

Repeat interval (hours): 0.25, 0.5, 1, 4

Error waiting time (hours): 24

Notify senders of messages in the queue every hours (0=off). 4

Size limit

☐ Limit the size of the queue

Maximum number of messages: 1000

Undeliverable messages

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

You can **Notify senders of messages in the queue every ... hours** whereby ... must be a full hour value. If you do not wish to inform the sender of an undeliverable message regularly, simply enter *0*. Even if you deactivate the regular notification of senders of non-forwarded email, the sender is, of course, still informed when the delivery of his email has finally failed and the email has been deleted from the server.

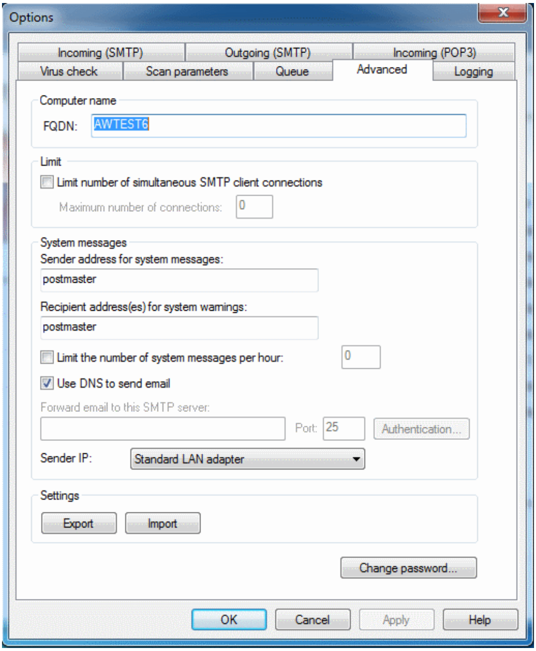
You can use the button **Reset to default values** to restore the default settings.

Size limit

To protect your mail server from Denial of Service attacks, you can limit the size of the queue. If the size limit is exceeded, no further emails are added to the queue.

Advanced

On the Advanced tab, you can change the global settings for G Data MailSecurity.



Computer name
FQDN: AWTEST6

Limit
☐ Limit number of simultaneous SMTP client connections
Maximum number of connections: 0

System messages
Sender address for system messages:
postmaster
Recipient address(es) for system warnings:
postmaster
☐ Limit the number of system messages per hour: 0
☑ Use DNS to send email
Forward email to this SMTP server:
Port: 25
Sender IP: Standard LAN adapter

Computer name

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

Limit

To limit the number of SMTP connections that G Data MailSecurity processes simultaneously, please check **Limit number of SMTP client connections** and enter a maximum number of connections. G Data MailSecurity then only permits the maximum number of connections that you specify. Using this function, you can adjust the mail filtering to the performance of the hardware that you are using for the mail gateway.

System messages

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

Settings

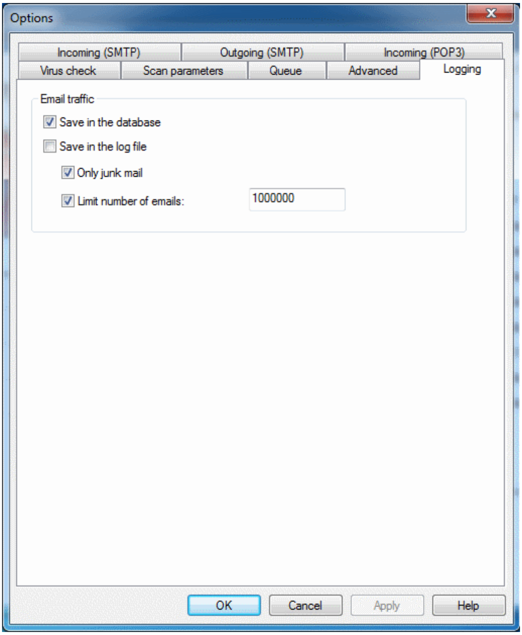
You can save the program option settings as an XML file using the **Import** and **Export** buttons, to make a backup and import them if necessary.

Change password

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

Logging

On the Logging tab you can set options for a statistical assessment of the server's mail traffic (**Save in the database**). To view the statistics, use the **Statistics** button in the **Status** panel of the main interface. Alternatively, select **Save in the log file** to save the logs in an external file (maillog.txt). By selecting **Only junk mail** or **limit number of emails** you can limit the size of the log file.



Email traffic

☑ Save in the database

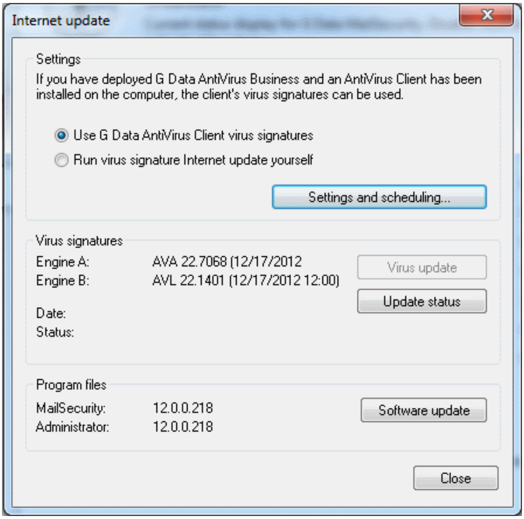
□ Save in the log file

☑ Only junk mail

☑ Limit number of emails: 1000000

Update

The Update window lets you configure G Data MailSecurity updates. Virus signatures and program data of G Data MailSecurity can be updated manually or automatically.



Internet update

Settings

If you have deployed G Data AntiVirus Business and an AntiVirus Client has been installed on the computer, the client's virus signatures can be used.

● Use G Data AntiVirus Client virus signatures

○ Run virus signature Internet update yourself

Settings and scheduling...

Virus signatures

Engine A: AVA 22.7068 (12/17/2012

Engine B: AVL 22.1401 (12/17/2012 12:00)

Date:

Status:

Virus update

Update status

Program files

MailSecurity: 12.0.0.218

Administrator: 12.0.0.218

Software update

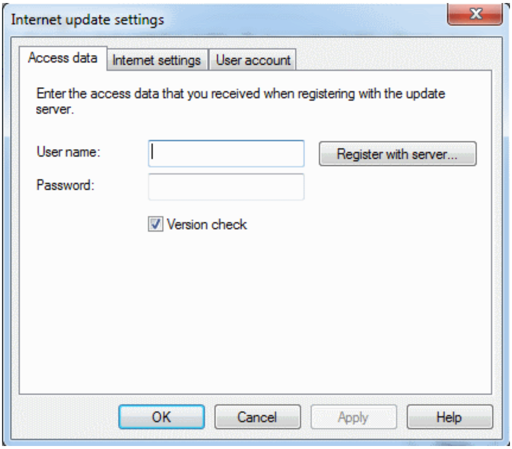
Close

Settings

If MailGateway is being operated as part of a G Data business solution, you can avoid duplicating the downloads by selecting **Use G Data AntiVirus Client virus signatures** and get them directly from the installed G Data Security Client. If you choose **Run virus signatures Internet update yourself**, G Data MailSecurity performs this operation autonomously. The **Settings and scheduling** button takes you to the area where you can enter all the settings required for manual and automatic updates.

Access data

Under Access data, enter the **user name** and **password** that you received when you registered G Data MailSecurity. The G Data Server will use this data to recognize you, so the virus signature update can be executed completely automatically. Click the **Register with server** button if you have not yet registered yet. Simply enter the registration number that can be found on your purchase certificate and your customer data and click **Send**. The login data (user name and password) will be displayed immediately. You should write down this data and keep it in a safe place. Of course, you need an Internet connection to log on to the server (and also for updating virus signatures via the Internet).



Enter the access data that you received when registering with the update server.

User name:

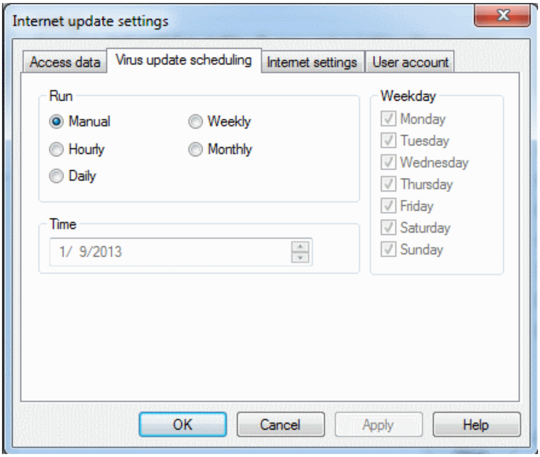
Password:

☑ Version check

Virus update scheduling

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

For **Daily** updates you can use the **Weekday** setting to specify if MailGateway should only carry out the update on working days or just every other day, or specifically on weekends only when it is not being used for work. To change the time and date under **Time**, simply highlight the item you wish to change (e.g., day, time, month, year) with the mouse and use the arrow keys or the small arrow symbols to scroll up and down chronologically.



Run
● Manual
○ Hourly
○ Daily
○ Weekly
○ Monthly

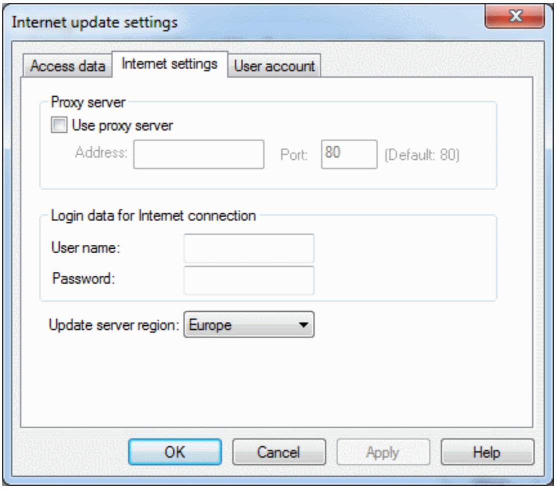
Time
1/ 9/2013

Weekday
☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday
☑ Sunday

Internet settings

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

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



Internet update settings

Proxy server

□ Use proxy server

Address:

Port: 80 (Default: 80)

Login data for Internet connection

User name:

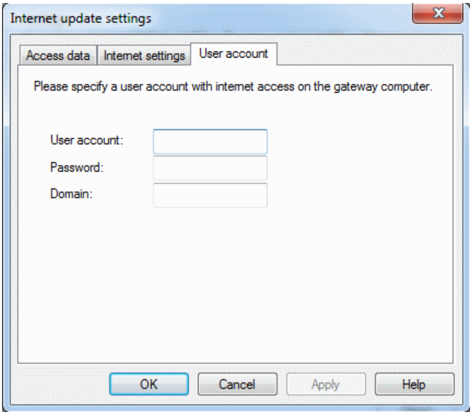
Password:

Update server region: Europe

User account

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

> **Warning**: Do not confuse the entries you make on the **Access data** and **User account** tabs.



Please specify a user account with internet access on the gateway computer.

User account:

Password:

Domain:

Virus signatures

The **Virus update** and **Update status** buttons enable you to start a virus signature update, regardless of the scheduled update checks.

Program files

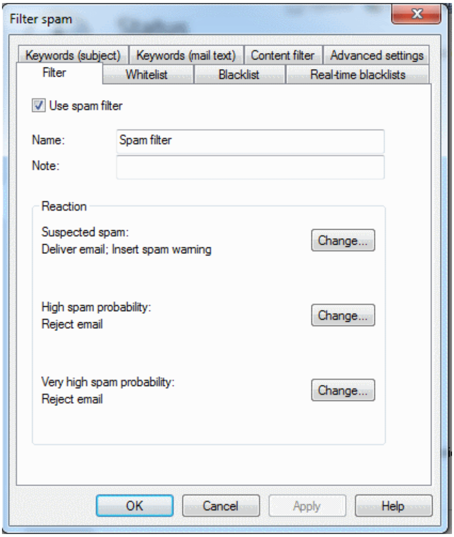
The **Software update** button lets you update the G Data MailSecurity program files as soon as changes or improvements have been made.

Spam filter

The spam filter provides you with an extensive range of settings to effectively block email with undesirable content or from undesirable senders (e.g. mass email senders). MailGateway checks for numerous email characteristics that are typical of spam. These characteristics are used to calculate a value reflecting the likelihood of the email being spam. To configure this process, multiple tabs are available.

Filter

You can give an individual name to each filter by entering it in the **Name** field. Add additional information that may be required in the **Note** field. Under **Reaction**, you can define how the spam filter should handle email that may possibly be spam. You can use the spam probability value calculated for the affected email by G Data MailSecurity to define three different levels of filtering.



☑ Use spam filter

Name: Spam filter

Note:

Reaction

Suspected spam:
Deliver email; Insert spam warning

High spam probability:
Reject email

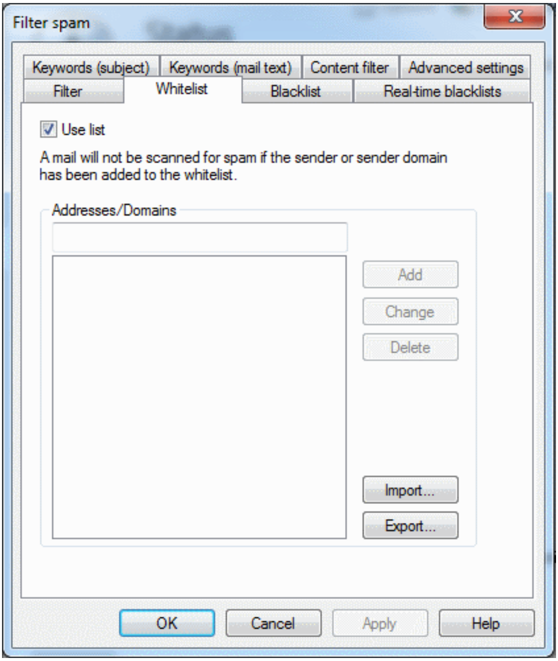
Very high spam probability:
Reject email

Suspected spam messages, which contain only a few spam characteristics, are not necessarily all spam, but can also be email newsletters or part of a mass emailing that is of interest to the recipient. In such cases, it is recommended that you inform the recipient that the email is suspected spam. **High spam probability** covers emails that contain many spam characteristics and that are rarely of interest to the recipient. **Very high spam probability** collects email that meets all the spam criteria. Such emails are rarely wanted, and rejecting email with these characteristics is recommended in most cases. Each of these three reactions can be customized.

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

Whitelist

Certain sender addresses or domains can be explicitly excluded from suspected spam by putting them on the whitelist. Simply enter the email address (e.g., *newsletter@gdata-software.com*) or Domain (e.g. *gdata-software.com*) that you want to exclude from suspected spam in the **Addresses/Domains** field, and G Data MailSecurity will never classify messages from that sender or sender domain as spam. You can use the **Import** button to insert predefined lists of email addresses or domains into the whitelist. Each address or domain must be listed on a separate line. A plain text file format is used for storing this list; you can create this list using an editor like Windows Notepad. You can also use the **Export** button to export whitelists as text files.

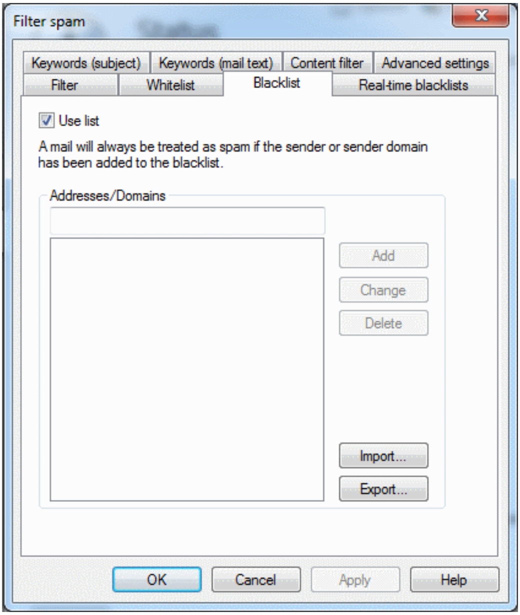


☑ Use list

A mail will not be scanned for spam if the sender or sender domain has been added to the whitelist.

Blacklist

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

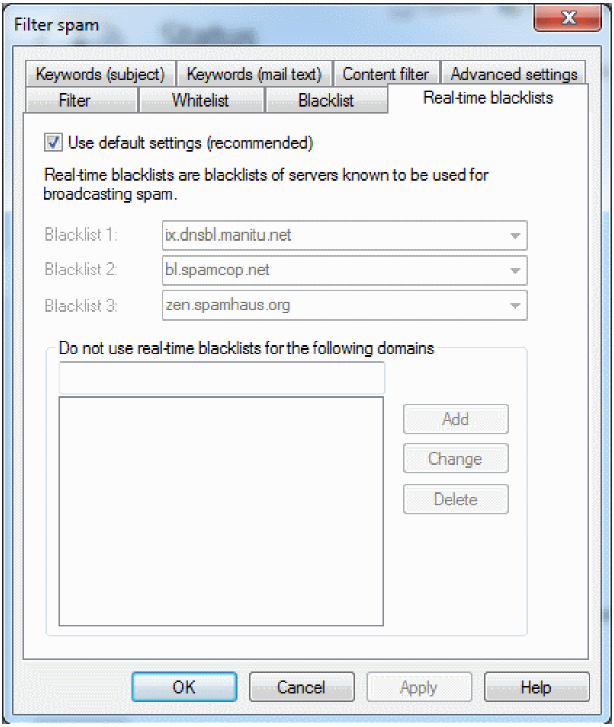


☑ Use list

A mail will always be treated as spam if the sender or sender domain has been added to the blacklist.

Real-time blacklists

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



☑ Use default settings (recommended)

Real-time blacklists are blacklists of servers known to be used for broadcasting spam.

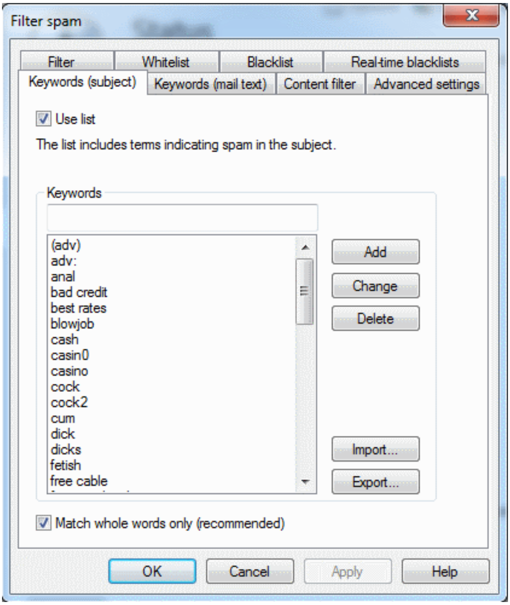
Blacklist 1: ix.dnsbl.manitu.net

Blacklist 2: bl.spamcop.net

Blacklist 3: zen.spamhaus.org

Keywords (subject)

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



☑ Use list

The list includes terms indicating spam in the subject.

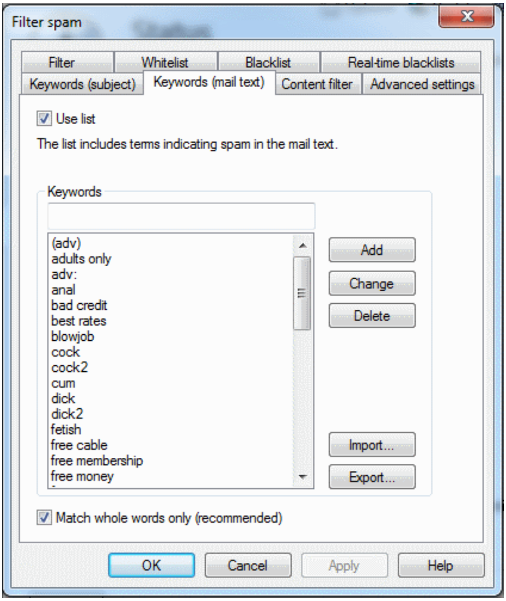
Keywords

(adv)
adv:
anal
bad credit
best rates
blowjob
cash
casin0
casino
cock
cock2
cum
dick
dicks
fetish
free cable

☑ Match whole words only (recommended)

Keywords (mail text)

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



Filter spam

☑ Use list

The list includes terms indicating spam in the mail text.

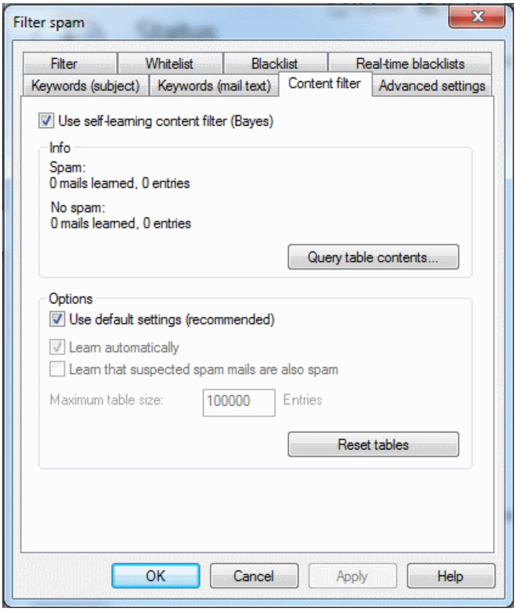
Keywords

(adv)
adults only
adv:
anal
bad credit
best rates
blowjob
cock
cock2
cum
dick
dick2
fetish
free cable
free membership
free money

☑ Match whole words only (recommended)

Content filter

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



☑ Use self-learning content filter (Bayes)

Info

Spam:
0 mails learned, 0 entries

No spam:
0 mails learned, 0 entries

Options

☑ Use default settings (recommended)

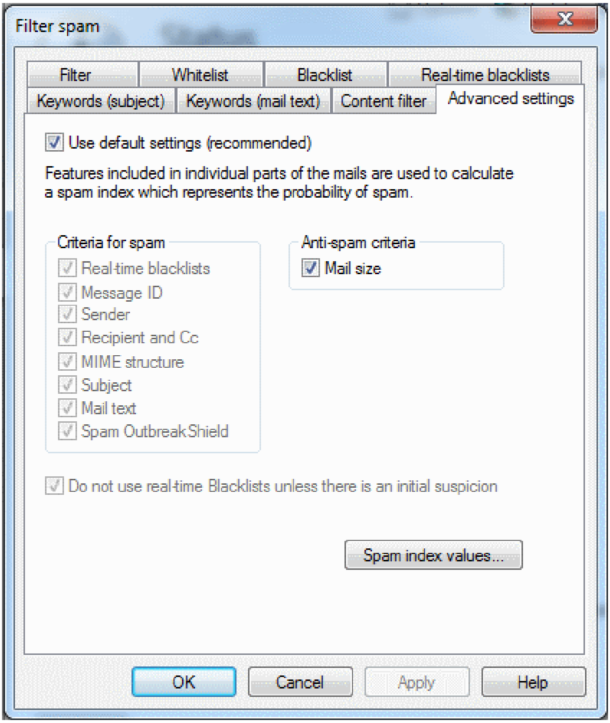
☑ Learn automatically

□ Learn that suspected spam mails are also spam

Maximum table size: 100000 Entries

Advanced settings

The Advanced settings tab can be used for very detailed changes to the G Data MailSecurity spam detection and to adapt it to the mail server environment. We recommend using the default settings here. Changes in the advanced settings should only be carried out if you know exactly what you are doing.



☑ Use default settings (recommended)

Features included in individual parts of the mails are used to calculate a spam index which represents the probability of spam.

Criteria for spam
☑ Real-time blacklists
☑ Message ID
☑ Sender
☑ Recipient and Cc
☑ MIME structure
☑ Subject
☑ Mail text
☑ Spam OutbreakShield

Anti-spam criteria
☑ Mail size

☑ Do not use real-time Blacklists unless there is an initial suspicion

Modules

Using G Data MailSecurity is generally self-explanatory and clearly structured. Using the various tabs on the left hand side of the Administrator interface, you can select the relevant module where you can carry out different actions, configure settings or review processes. The following modules are available:

Status

Filter

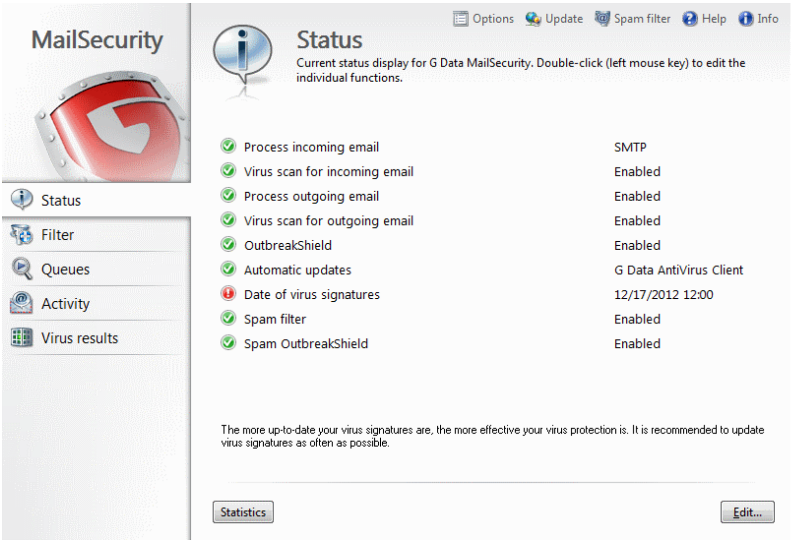
Queues

Activity

Virus results

Status

In the Status module, you will find basic information about the current status of your system and MailGateway.



Status

Current status display for G Data MailSecurity. Double-click (left mouse key) to edit the individual functions.

✓	Process incoming email	SMTP
✓	Virus scan for incoming email	Enabled
✓	Process outgoing email	Enabled
✓	Virus scan for outgoing email	Enabled
✓	OutbreakShield	Enabled
✓	Automatic updates	G Data AntiVirus Client
!	Date of virus signatures	12/17/2012 12:00
✓	Spam filter	Enabled
✓	Spam OutbreakShield	Enabled

The more up-to-date your virus signatures are, the more effective your virus protection is. It is recommended to update virus signatures as often as possible.

As long as the G Data MailSecurity virus protection is optimally configured, you will see a green icon to the left of the listed entries.

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

By double-clicking the relevant entry (or by selecting the entry and clicking the **Edit** button), you can directly switch to the relevant module. As soon as you have optimized the settings for a component with a warning icon, the icon will turn green again. The following entries are available:

- **Process incoming email**: Processing incoming email ensures that email is checked by the MailGateway before being forwarded to the recipient. If you double-click this entry, the corresponding settings window appears (menu bar: **Options** > **Incoming (SMTP)**) and you can configure incoming email processing.
- **Virus scan for incoming email**: Scanning incoming email stops infected files from reaching your network. If you double-click this entry, the corresponding settings window appears (menu bar: **Options** > **Virus check**) and you can configure incoming email scanning.
- **Process outgoing email**: Processing outgoing email ensures that email is checked by the MailGateway before being forwarded to the recipient. If you double-click this entry, the corresponding settings window appears (menu bar: **Options** > **Outgoing (SMTP)**) and you can configure incoming email processing.
- **Virus scan for outgoing email**: Scanning outgoing email stops infected files from being sent out from your network. If you double-click this entry, the corresponding settings window appears (menu bar: **Options** > **Virus check**) and you can configure outgoing email scanning.
- **OutbreakShield**: OutbreakShield lets you detect and neutralize malware in mass mails before updated signatures are available. OutbreakShield uses the Internet to monitor increased volumes of suspicious email, enabling it to close the window between the mass email outbreak and its containment with specially adapted signatures, practically in real time.
- **Automatic updates**: Virus signatures can be updated separately but you should enable the automatic updates option. If you double-click this entry, the corresponding settings window appears (menu bar: **Internet update**) and you can configure the update frequency.
- **Date of virus signatures**: Your virus protection is only secure with the most recent updates. You should update the virus signatures as often as possible and automate this process. If

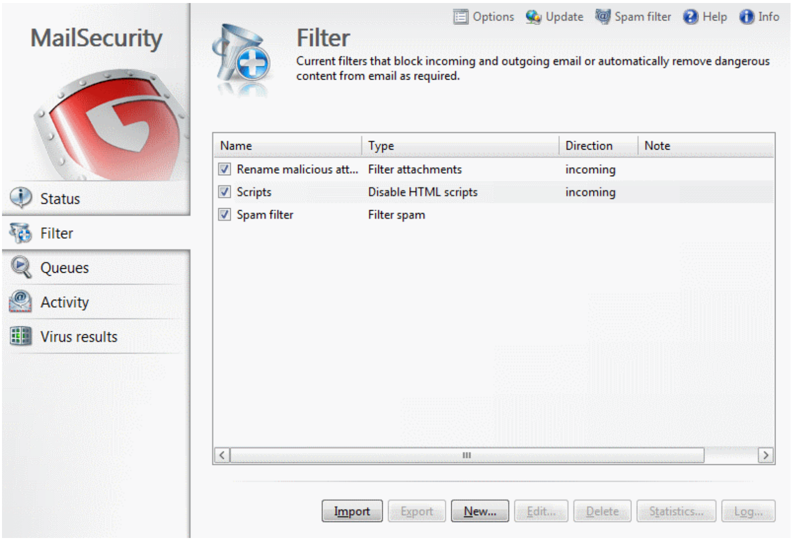
you double-click this entry, the corresponding settings window appears (menu bar: **Internet update**) and you can also perform an Internet update directly (regardless of possible update schedules).

- **Spam filter**: The **Spam filter** offers extensive settings options which effectively block email with unwanted content or email from unwanted senders (e.g. mass email senders).
- **Spam OutbreakShield**: The Spam OutbreakShield can detect and eliminate mass email quickly and safely. Before email is retrieved from the Internet, Spam OutbreakShield gets info on particular increased volumes of suspicious email and does not allow them to reach the recipient's inbox.

If you installed the option for Statistical assessment, the Status panel will also show a Statistics button. It will show statistical information about the mail server and can be configured through **Options** > **Logging**.

Filter

In the Filter area, you can use convenient filters to block incoming mail or automatically remove potentially dangerous content from email. The respective filters are shown in the list under Filters and can be enabled or disabled as required by ticking the checkbox to the left of the respective entry.



Current filters that block incoming and outgoing email or automatically remove dangerous content from email as required.

Name	Type	Direction	Note
☑ Rename malicious att...	Filter attachments	incoming	
☑ Scripts	Disable HTML scripts	incoming	
☑ Spam filter	Filter spam		

- **Import**: Import filter XML files to restore a backup or reuse filters from other computers.
- **Export**: Individual filters with your settings can be exported as an XML file to be backed up or to be reused on other computers. To export multiple filters, click them while holding the Ctrl key.
- **New**: You can create new filter rules with the **New** button. When you create a new filter, a selection window appears in which you can specify the basic filter type. All of the other details about the filter can be created using a wizard, which will guide you through that filter type. This is a convenient way to create filters for every imaginable type of threat.
- **Edit**: You can edit existing filters with the **Edit** button.
- **Delete**: To permanently delete a filter, click the relevant filter once to highlight it and then click the **Delete** button.
- **Statistics**: You can check statistical information for every filter.

- **Log**: For the **spam filter**, there is a log with a list of emails rated as potential spam. The log also shows which criteria were responsible for the spam rating (spam index values). In the event of an incorrect spam rating, you can inform the OutbreakShield server online that there has been a false detection (false positive). The mail is then rechecked by OutbreakShield and - if it really was falsely detected as spam - it is then reclassified as harmless. In doing so, only a checksum is transferred and not the content of this email.

> Your network is continuously protected from virus infections, irrespective of individual filter rules, because G Data MailSecurity checks incoming and outgoing mail in the background. Filter rules are designed to protect your email accounts from unsolicited mail, spam and unsafe scripts, and to minimize potential virus sources even before virus detection by G Data MailSecurity.

General filter functions

For all filter types, you can enter a name for the filter under **Name**. You can specify internal notes and comments for the filter concerned under **Note**. Under **Direction**, a filter rule can be defined to apply only to **incoming email**, only to **outgoing email**, or both directions.

In the **Reaction** section, you can specify how email should be handled when it meets the filter criteria (as soon as it is identified as spam). A message text can be customized for the options **Notify sender** and **Send alert to the following persons**. To do so, simply click the **...** button to the right of the respective reaction. You can also use wildcards to copy information relating to the rejected email into the notification text. In the text you define for the **Subject** and the **Email text**, the following wildcards (defined using a percentage symbol followed by a lower case letter) are available:

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

- %i > **Sender IP**

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

Filter read receipt

This filter deletes requests for a read receipt for incoming and/or outgoing e-mails.

Disable HTML scripts

This filter disables scripts in the HTML part of an email. Scripts that make sense on a web page may be rather irritating when they are integrated into an HTML email. In some cases, HTML scripts are also used to actively infect computers, while scripts even have the option of running in an email preview.

Disable external references

Many newsletters and product announcements in HTML format contain references, which are only executed or displayed if the email is opened. These can be images that were not sent with the email but are loaded automatically via a hyperlink. Not all of these external resources are just harmless pictures: they can also be malicious routines. It makes sense to disable these references. Disabling them does not affect the actual email text.

Greylist filter

Greylisting is an extremely effective method to reduce incoming spam emails. As soon as an email comes into the system, the greylist filter sends back a request to the sending server to resend the message. As most spam senders do not maintain an email queueing system, the message will not be resent by the spammer.

- **Waiting times**: The waiting time determines how long suspicious emails should be held back. Once this time has elapsed, the email will be passed through if it has been resent. The sender will then be removed from the greylist and added to the whitelist. Any emails from this sender will no longer be dealt with by the greylist filter and will be delivered immediately.

- **Lifetimes**: To keep the whitelist constantly up to date, a sender address will only remain on the whitelist for a certain amount of time if no mail has been received from this sender. After this, the sender will be removed from the whitelist automatically. Example: in order to receive a monthly newsletter, set lifetimes value (TTL) to 30 days to permanently keep the sender address on the whitelist.

> The greylist filter is only available if G Data MailSecurity's **spam filter** is active and if an SQL database has been installed on the server.

Filter attachments

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

Under **File extensions** you can list the file extensions to which you would like to apply the filter. This lets you list all executable files (e.g. EXE, COM) in one filter, and have another filter for other formats (e.g. MPEG, AVI, MP3, JPEG, JPG, GIF) if their file size would overload the mail server. You can also filter archive files (e.g. ZIP, RAR or CAB). Separate all file extensions in a filter group by a semicolon, e.g. *.exe; *.dll. Under Mode, indicate whether you would like to allow the file endings under File extensions (**Only allow specified attachments**) or prohibit them (**Filter specified attachments**).

The function **Also filter attachments in embedded email** ensures that the filtering performed under File extensions also applies to email messages that are themselves being forwarded as email attachments. This option should be activated. Choosing **Only rename attachments** has the effect that filtered attachments are not deleted automatically but only renamed. This is not only recommended for executable files (such as EXE and COM) but also for Microsoft Office files that may contain executable scripts and macros. Renaming an attachment makes it impossible to open it simply by clicking it. Instead, the user must first save (and possibly rename) the attachment before it can be used. If **Only rename attachments** is not ticked, filtered attachments are deleted directly.

Under **Suffix**, you can enter a character string with which the file extension should be extended: *.exe_danger, for instance. In this manner, the execution of a file by simple clicking is prevented. Under **Insert message in mail text** you can inform the recipient of the filtered email that an attachment was deleted or renamed based on a filter rule.

Content filter

You can use the content filter to easily block email that contains certain subjects or text. To do this, under **Regular printout** (regular expression) simply enter the keywords and expressions that G Data MailSecurity should respond to. You can use the **New** button on the right to enter text that triggers a filter action. It is possible to use the logical operators **AND** and **OR** to link text components with each another. Under **Search scope** specify which parts of an email are to be scanned for these expressions.

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

You can also combine any search terms of your choice without the input help under Regular expression. To do so, simply enter the search terms and link them using a logical operator. *Or* corresponds to the vertical line | (Shift + \). *And* corresponds to the ampersand & (Shift + 6).

Sender filter

You can use the sender filter to block email coming from certain senders. To do this, under **Addresses/Domains**, simply enter the email addresses or domain names which G Data MailSecurity should filter. Use a semicolon to separate multiple entries. You can also automatically filter out email with no sender.

Recipient filter

You can use the recipient filter to filter emails for certain recipients. To do this, under **Addresses/Domains**, simply enter the email addresses or domain names which G Data MailSecurity should filter. Use a semicolon to separate multiple entries. You can also automatically filter out emails with a blank recipient field (i.e. emails that only have BCC and/or CC recipients).

Filter spam

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

IP filter

The IP filter prevents the receipt of email sent from certain servers. The filter can function in blacklist or whitelist mode. Under **Name** and **Note**, enter information about why you want to block the respective IP addresses and then enter every individual IP address under **IP addresses**. Click **Add** to add the IP address to the list of blocked IP addresses. You can also export the list of IP addresses as a text file or import a text file with IP addresses.

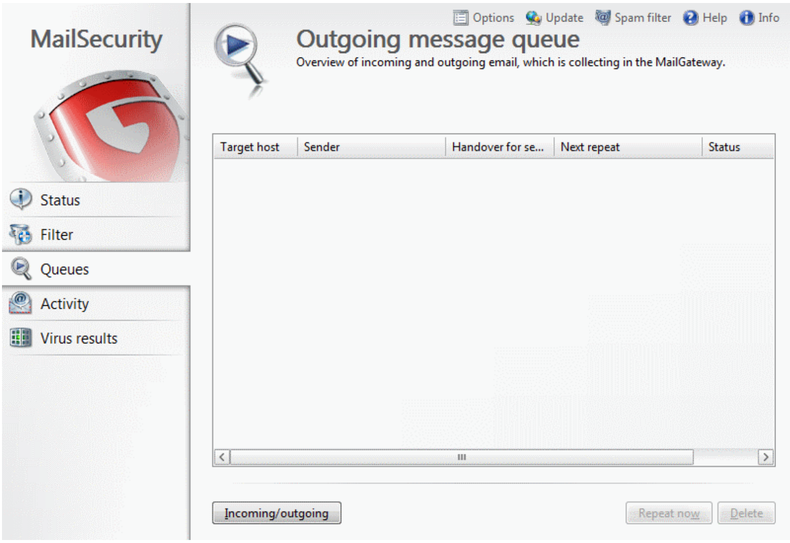
Language filter

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

Queues

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

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



Outgoing message queue

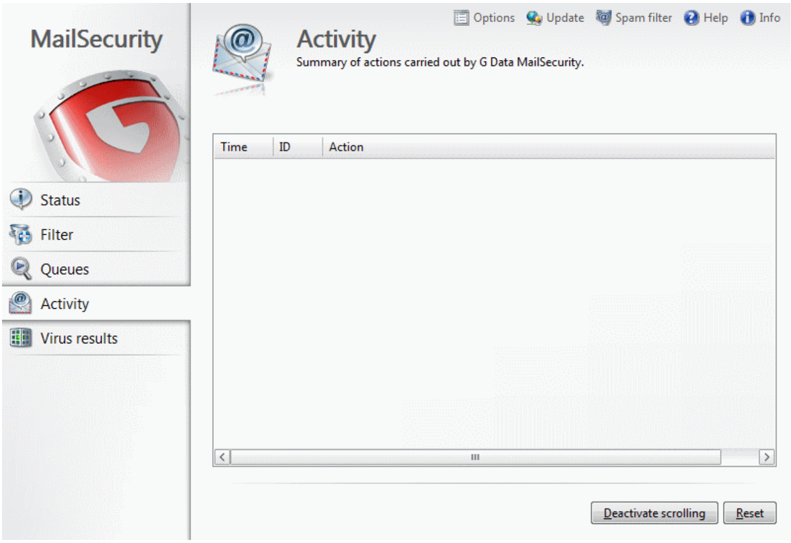
Overview of incoming and outgoing email, which is collecting in the MailGateway.

Target host	Sender	Handover for se...	Next repeat	Status

Activity

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

> You can use the **ID** to discover multiple actions for one email. Transactions with the same ID always belong together (e.g., 12345 Download email, 12345 Process email, 12345 Send email).

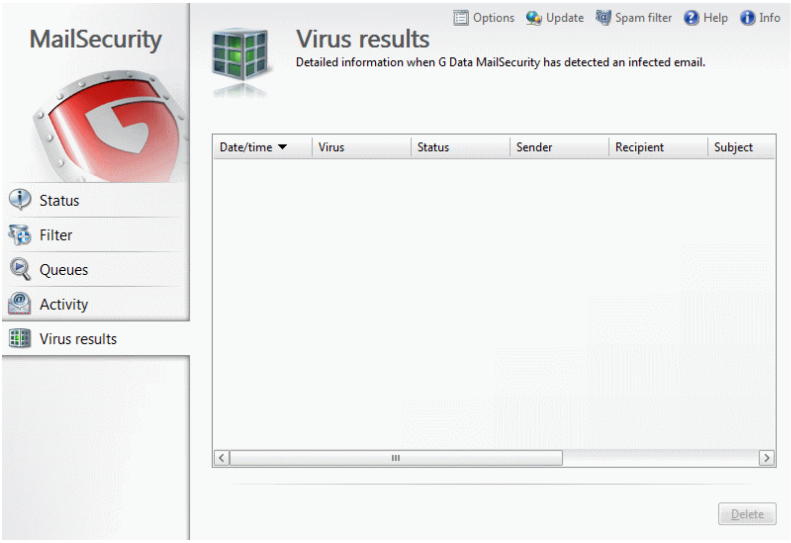


Activity

Summary of actions carried out by G Data MailSecurity.

Virus results

In the Virus results module, you get detailed information about when G Data MailSecurity detected an infected email, which measures were taken, the type of virus that the email contained, and the actual sender and recipient of the affected email. Use **Delete** to remove the selected virus alert from the virus results list.

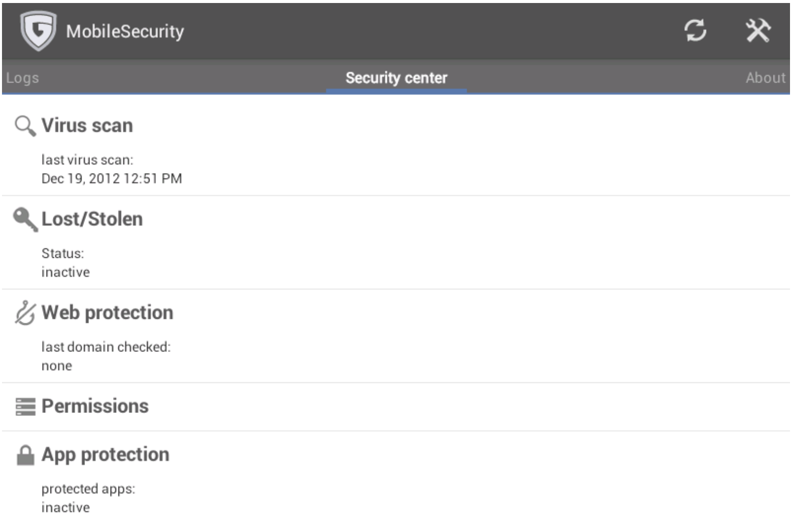


Virus results

Detailed information when G Data MailSecurity has detected an infected email.

G Data MobileSecurity

G Data offers a specially tailored business version of G Data MobileSecurity for Android devices to make use of G Data's Mobile Device Management features. Installation takes place **through G Data Administrator**.



MobileSecurity

Logs | Security center | About

Virus scan

last virus scan:
Dec 19, 2012 12:51 PM

Lost/Stolen

Status:
inactive

Web protection

last domain checked:
none

Permissions

App protection

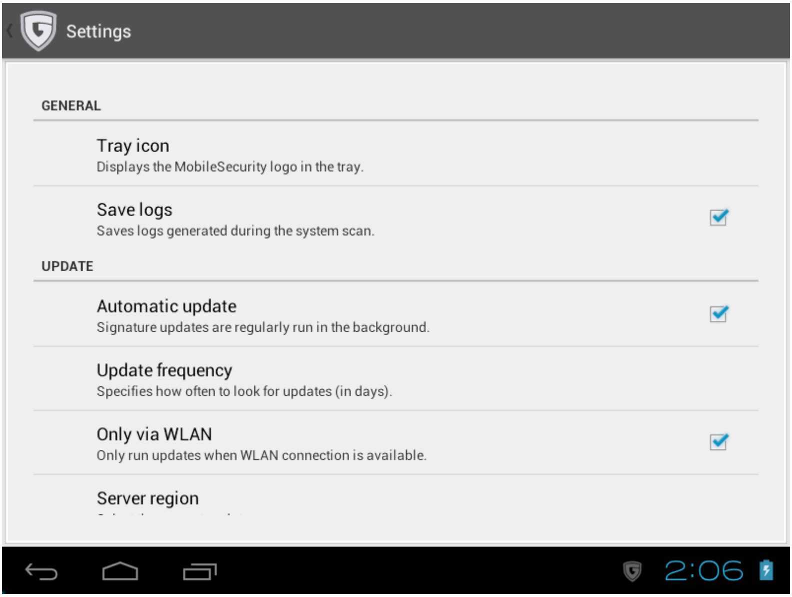
protected apps:
inactive

The Security center of G Data MobileSecurity provides access to all features. By swiping to the left, the **Logs** module can be opened. Swiping to the right reveals version info. The buttons in the top right corner of the screen allow you to check for updates and open the **Settings** menu.

Configuring G Data MobileSecurity

Settings

Most of the settings for G Data MobileSecurity can be managed through the **Mobile settings** module of G Data Administrator. However, on the device itself there is also the possibility to configure some features.



Settings

GENERAL

Tray icon
Displays the MobileSecurity logo in the tray.

Save logs ☑
Saves logs generated during the system scan.

UPDATE

Automatic update ☑
Signature updates are regularly run in the background.

Update frequency
Specifies how often to look for updates (in days).

Only via WLAN ☑
Only run updates when WLAN connection is available.

Server region

General

Tray icon: Displays the G Data MobileSecurity icon in the app tray.

Save logs: Saves scan logs to be viewed in the Logs module.

Update

Automatic update (also in **Mobile settings**): Virus signatures are updated automatically in the background.

Update frequency (also in **Mobile settings**): Specify the update frequency for signature updates (**1**, **3**, **7**, **14**, or **30** days).

Only via WLAN (also in **Mobile settings**): Only update virus signatures when Wi-Fi connectivity is available.

Server region: Select the nearest update server (not used when Remote Administration is enabled).

Virus scan

Periodic virus scan (also in **Mobile settings**): Opens the scan settings of the **Virus scan** module.

Web protection

Only with WLAN (also in **Mobile settings**): Only scan websites for phishing when Wi-Fi connectivity is available.

Remote administration

Allow remote administration: Allow MobileSecurity to be managed by G Data ManagementServer.

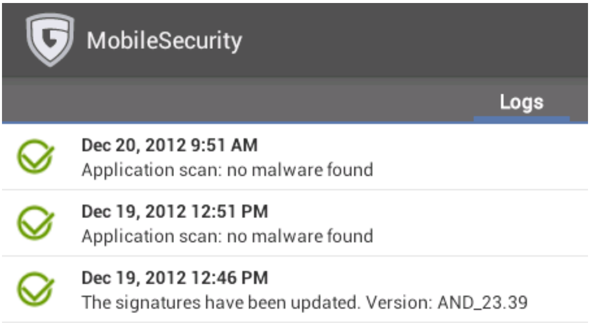
Server address: Enter the IP address or server name of the G Data ManagementServer.

Device name: Enter a name to identify the device with.

Password: Enter the password that is used to authenticate the device with G Data ManagementServer (defined in G Data Administrator's **Server settings** window).

Logs

The Logs view allows you to check on recent logs, such as scan reports and signature update reports. Select a log to view its details. Logging can be enabled or disabled in the **Settings** module.



Dec 20, 2012 9:51 AM
Application scan: no malware found

Dec 19, 2012 12:51 PM
Application scan: no malware found

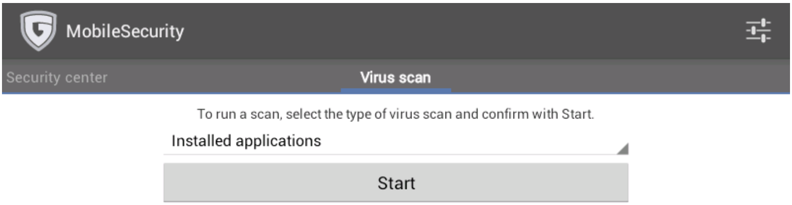
Dec 19, 2012 12:46 PM
The signatures have been updated. Version: AND_23.39

Modules

Virus scan

To carry out a comprehensive manual malware scan, the **Virus scan** option allows you to choose between two scan methods:

- **Installed applications**: This scan compares the list of installed applications to a list of known malware. If any malware is found on your device, MobileSecurity will offer you the possibility to remove it.
- **System (full scan)**: The full scan checks your complete smartphone storage for malware. This assists in the early detection of malware, for example by detecting malicious apps on an SD card before they are even installed.



To run a scan, select the type of virus scan and confirm with Start.

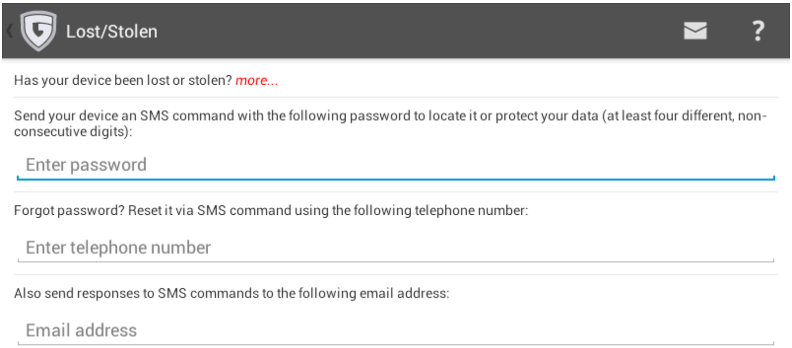
Installed applications

Select the **Settings** icon in the top right corner to configure automatic and periodic scans. Note that these settings can also be remotely managed through G Data Administrator's **Mobile settings** module:

- **Automatic scan**: Enable an automatic scan for newly installed applications.
- **Periodic virus scan:** Enable a periodic scan.
- **Battery save mode**: Allow a virus check even when the device is in power saving mode.
- **Scan during load process**: Run the periodic scan only when the device is being charged.
- **Scan frequency**: Define how often the periodic scan will be run (once every **1**, **3**, **7**, **14** or **30** days).
- **Type of virus scan**: Choose between a quick scan of installed apps only or a system scan.

Lost/Stolen

To protect lost or stolen devices, MobileSecurity supports various measures that can be remotely activated by SMS. The first time you open the Lost/Stolen menu, you will be prompted to enter a **password**, **telephone number**, and **email address**.



Has your device been lost or stolen? *more...*

Send your device an SMS command with the following password to locate it or protect your data (at least four different, non-consecutive digits):

Enter password

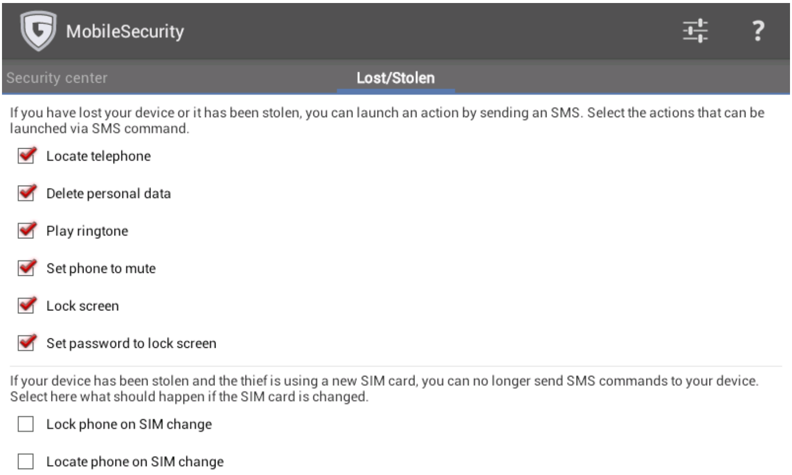
Forgot password? Reset it via SMS command using the following telephone number:

Enter telephone number

Also send responses to SMS commands to the following email address:

Email address

The password (a PIN code) is used as an identification via SMS, to ensure that no unauthorised commands can be sent to the device. An additional security measure is the telephone number. You can remotely reset your password only from the number that is entered here . Finally, enter an email address to which the device should send responses if SMS commands are used. Tap **Done** in the top left corner of the screen to save your settings. If necessary, confirm the added device administrator permissions for MobileSecurity by tapping **Activate**. These settings can later be changed by activating the **Settings** icon in the top right corner.



If you have lost your device or it has been stolen, you can launch an action by sending an SMS. Select the actions that can be launched via SMS command.

☑ Locate telephone

☑ Delete personal data

☑ Play ringtone

☑ Set phone to mute

☑ Lock screen

☑ Set password to lock screen

If your device has been stolen and the thief is using a new SIM card, you can no longer send SMS commands to your device. Select here what should happen if the SIM card is changed.

□ Lock phone on SIM change

□ Locate phone on SIM change

The Lost/Stolen settings screen allows you to choose different security settings. Each one can be activated by sending a specially crafted SMS message from the telephone number entered in the Settings window, including the specified password. The following options are available:

- **Locate telephone**: The device will send its location to the email address specified in the Settings window. To activate this feature, send an SMS containing the text *password* **locate**.
- **Delete personal data:** The device will be reset to its factory settings. All personal data will be wiped. To activate this feature, send an SMS containing the text *password* **wipe**.
- **Play ringtone**: The device will play a ringtone continuously. This will assist in locating lost devices. To activate this feature, send an SMS containing the text *password* **ring**.
- **Set phone to mute**: If you do not want the device to call attention to itself with ringtones or other signals, it can be muted. This does not include the ringtone that is used to locate lost devices. To activate this feature, send an SMS containing the text *password* **mute**.
- **Lock screen**: The device screen can be locked to prevent the device from being used. To activate this feature, send an SMS containing the text *password* **lock.** If no lock screen password has been set, the password from the Settings window will be used.

- **Set password to lock screen**: Set a password to unlock the phone if the lock screen feature has been enabled. To activate this feature, send an SMS containing the text *password* **set device password:** *devicepassword*. Make sure to send the **lock** command to lock the device after setting the password.

Additionally, you can specify what should happen to the device if the SIM card is changed. Be sure to disable these options prior to any SIM card changes that may need to be carried out.

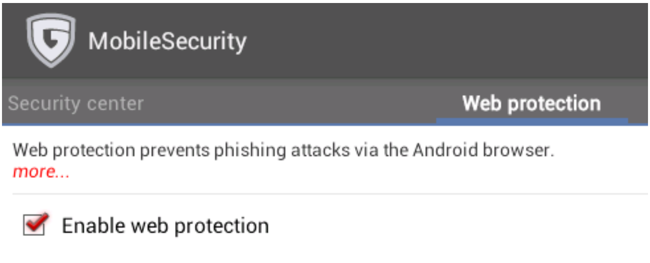
- **Lock phone on SIM change**: When the SIM card that was in the device when MobileSecurity was activated is changed or removed, access to the device will be blocked completely. When the original SIM card is returned, the device will be unblocked.
- **Locate phone on SIM change**: When the SIM card is changed or removed, the current position of the device will be emailed to the address specified in the Settings window.

To remotely reset your password, send an SMS from the phone number that you specified earlier containing the text **remote password reset**: *password*.

Web protection

The Web protection module prevents phishing attacks. It blocks phishing websites from being opened in the Android browser. Since some data traffic is required to check the list of phishing websites, the Web protection module can be configured in the **Settings** menu to only look up websites when there is Wi-Fi connectivity.

Web protection and its connectivity setting can also be managed centrally through G Data Administrator's **Mobile settings**.

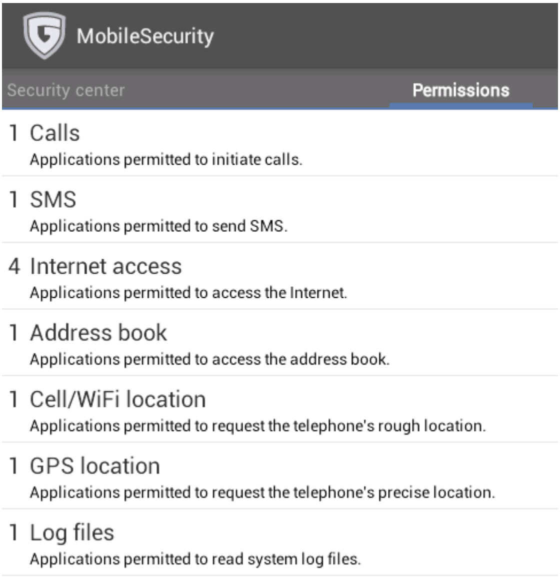


Web protection prevents phishing attacks via the Android browser.
more...

☑ Enable web protection

Permissions

The Permissions module provides an at-a-glance overview of permission usage across all installed apps. To quickly check which apps have requested permissions for a specific action, tap the action (such as **Calls**, **SMS**, or **Address book**). In the overview, you can directly uninstall apps if you decide they form an unnecessary risk.



1 Calls
Applications permitted to initiate calls.

1 SMS
Applications permitted to send SMS.

4 Internet access
Applications permitted to access the Internet.

1 Address book
Applications permitted to access the address book.

1 Cell/WiFi location
Applications permitted to request the telephone's rough location.

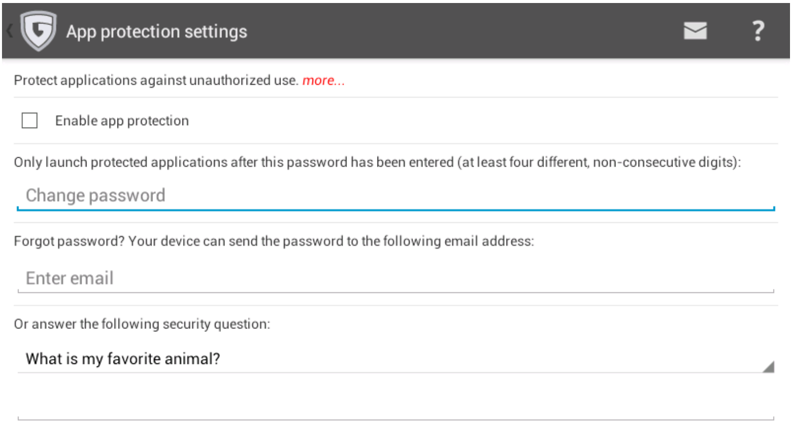
1 GPS location
Applications permitted to request the telephone's precise location.

1 Log files
Applications permitted to read system log files.

-

App protection

App protection allows you to block certain apps from being used on the device. Using password protection, apps like Play Store can be blocked. The first time you open the App protection module, you will be prompted to enter a **password**, **email address**, and **security question**.



Protect applications against unauthorized use. more...

□ Enable app protection

Only launch protected applications after this password has been entered (at least four different, non-consecutive digits):

Change password

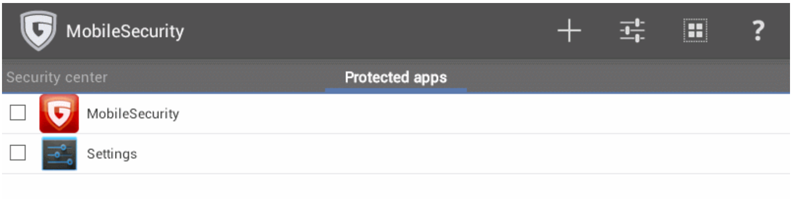
Forgot password? Your device can send the password to the following email address:

Enter email

Or answer the following security question:

What is my favorite animal?

The password (a PIN code) is used to access blocked apps. You can choose to enter an e-mail address to which the password will be sent in case you forget it, or define a security question and answer. Click **Done** in the top left corner to save the settings and check **Enable app protection** to activate the option. The settings can be changed at any time by tapping the **Settings** icon in the top right corner.



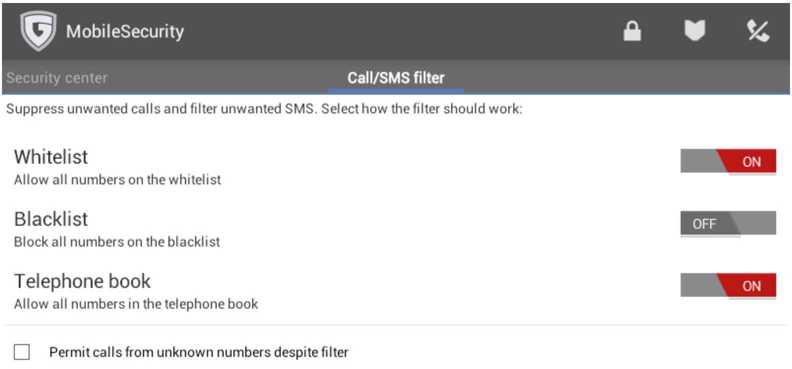
□ MobileSecurity

□ Settings

The main panel of App protection shows you the list of protected apps. To add an app, tap the **+** button in the top right corner. You can select apps using different views: **Recommended**, **Downloaded**, and **All**. Select an app to add it to the list. It is automatically protected and will ask for the password when it is launched. To remove an app from the list, select it and tap the **Done** button in the top left corner.

Call/SMS filter

The Call/SMS filter consists of two separate options. You can choose to enable a **blacklist** or **whitelist** approach to block or allow numbers that are on the list. Separately, you can enable the **Telephone book** option to allow all numbers in the telephone book, regardless of black- or whitelist. Calls from unknown numbers can be allowed or blocked by ticking or unticking the checkbox **Permit calls from unknown numbers despite filter**.



Suppress unwanted calls and filter unwanted SMS. Select how the filter should work:

Whitelist
Allow all numbers on the whitelist
ON

Blacklist
Block all numbers on the blacklist
OFF

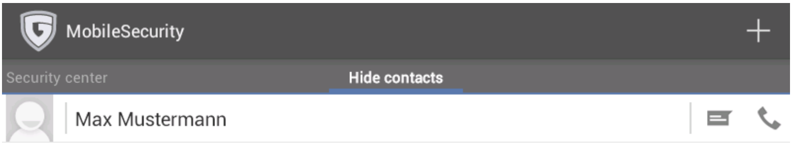
Telephone book
Allow all numbers in the telephone book
ON

□ Permit calls from unknown numbers despite filter

To view the black- or whitelist, tap the **Lock** icon. To add a number to the list, tap the **+** icon. Phone numbers can be added from the address book or call history. To view the address book, tap the **address book** icon. For a log of suppressed calls and SMS messages, tap the **phone** icon in the top right corner.

Hide contacts

Contacts and their incoming communication can be hidden. By moving them to a separate G Data account, the Hide contacts module effectively blocks access to the contact and all its communication.



Active the Hide contacts option to see a list of currently hidden contacts. To add a contact, tap the **+** button. You can select any contact from your address book or call history. After adding a contact, tap its name to edit the protection options. Incoming calls and messages can be intercepted by selecting **Hide incoming communication**. To hide the contact from the address book, select **Hide contacts**. Intercepted messages can also be viewed in the contact screen by selecting **Message history** or **Call history**. To unhide a contact and move it back to the regular address book, tap and hold the contact's name and choose **Delete entry**.

Troubleshooting (FAQ)

Installation

After client installation, some applications run significantly slower than before

The G Data monitor oversees all file accesses in the background and performs virus checks. 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 resolved 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 **Support**.

> You can also increase performance by using just one engine rather than two for virus checks. This primarily applies to older systems and can be defined in the **Client settings**.

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

To register the software after the installation, open **Internet update** under **Start** > **All Programs** > **G Data** > **G Data 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 the registration number in the license document (MediaPack) or order confirmation. In case of doubt, contact your dealer or the relevant distributor.

On entering the registration number, your product is activated. The access data generated is displayed following successful registration. **Be sure to make a note of these access data!** Following successful registration, it is no longer possible to re-enter the license 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 lowercase letter "l" (for Lima). The same applies to: "B" and "8", "G" and "6", "Z" and "2".

> If you have purchased G Data ClientSecurity, G Data EndpointProtection, or PatchManager as add-on module, and did not activate it on installation, the Firewall, PatchManager, and PolicyManager tabs are only enabled following successful activation. Until then, only the G Data AntiVirus Business functions are available.

MailSecurity, Exchange Server 2000 and AVM Ken!

If you are using AVM Ken! and would like to install G Data MailSecurity on the same computer as the Ken!-server, our **support team** can supply detailed instructions.

If you are using Exchange Server 2000 and would like to install G Data MailSecurity on the same computer as the Exchange Server, or you would like to change the ports for incoming and outgoing mail on the Exchange server, our **support team** can supply detailed instructions.

Error messages

Client: "Program files were changed or are corrupt"

In order to ensure optimal 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 listed in the **Reports** module. Delete the report and download the current update of the program files (G Data Client) from the G Data server. Subsequently, perform an update of the program files on the affected clients. Please contact our **support team** if the error occurs again.

Client: "The virus database is corrupt"

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 listed in the **Reports** module. Delete the report and download the current update of the virus database from the G Data server. Then, perform an update of the virus database on the affected clients. Please contact our **support team** if the error occurs again.

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

If you receive the error message "You must have at least Microsoft Exchange Server 2007 SP1", the minimum requirements for installing the G Data MailSecurity Exchange plugin have not been fulfilled. For an installation, Microsoft Exchange 2007 with Service Pack 1 is required. It must be installed before G Data MailSecurity. See also **Installation** and **System requirements**.

Using Linux

Linux file server clients: No connection with the G Data ManagementServer has been made / signatures are not being updated

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

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

You should receive the following response:

```
...     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 administrator (root) on the Linux computer.

2 View the log files: 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 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: **etc/gdata/avclient.cfg** is the configuration file for the remote client **avclient**. Check whether the address of the ManagementServer is entered correctly. If not, delete the incorrect entry and enable the Linux client again via the G Data Administrator, or enter the address of the G Data ManagementServer directly.

5 Test your authorization: Virus protection for Samba authorization is enabled with the entry **vfs objects = gdvfs** in the Samba configuration file **/etc/samba/smb.conf**. If the entry is in section **[global]**, protection for all shares is enabled. If the line is in another section, the protection only applies to the corresponding share. You can comment out the line for test purposes (by entering the "#" symbol at the start of the line) to see whether access functions without virus protection. If not, 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 in use. 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**.

Other

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

The **Last access** column in the **Clients** module contains the date on which the client last reported to G Data ManagementServer. In the default setting, the clients report to G Data 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 G Data ManagementServer. Check the network and port forwarding 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 7167/7169 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. 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.

My mailbox was moved to the quarantine

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

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

Installing G Data 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 ManagementServer has already been installed. To do this, alter the following registry entries:

HKEY_LOCAL_MACHINE\SOFTWARE\G DATA\AVK ManagementServer\ComputerName

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

Enabling clients in 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 G Data Administrator with their IP address. This can be done either manually or by **Active Directory Synchronization**.

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.

Storage locations and paths

G Data Security Client virus signatures

- Windows XP / Server 2003 / Server 2003 R2: C:\Program Files \Common Files\G DATA\AVKScanP\AVAST5 or BD
- Windows Vista / Windows 7 / Windows 8 / Server 2008 / Server 2008 R2 / Server 2012: C:\Program Files (x86)\Common Files \G DATA\AVKScanP\AVAST5 or BD

G Data ManagementServer virus signatures

- Windows XP / Server 2003 / Server 2003 R2: C:\Documents and Settings\All Users\Application Data\G DATA\AntiVirus ManagementServer\Updates
- Windows Vista / Windows 7 / Windows 8 / Server 2008 / Server 2008 R2 / Server 2012: C:\ProgramData\G DATA\AntiVirus ManagementServer\Updates

G Data Security Client quarantine

- Windows XP / Server 2003 / Server 2003 R2: C:\Program Files \Common Files\G DATA\AVKScanP\QBase
- Windows Vista / Windows 7 / Windows 8 / Server 2008 / Server 2008 R2 / Server 2012: C:\Program Files (x86)\Common Files \G DATA\AVKScanP\QBase

G Data ManagementServer quarantine

- Windows XP / Server 2003 / Server 2003 R2: C:\Documents and Settings\All Users\Application Data\G DATA\AntiVirus ManagementServer\Quarantine
- Windows Vista / Windows 7 / Windows 8 / Server 2008 / Server 2008 R2 / Server 2012: C:\ProgramData\G DATA\AntiVirus ManagementServer\Quarantine

MMS databases

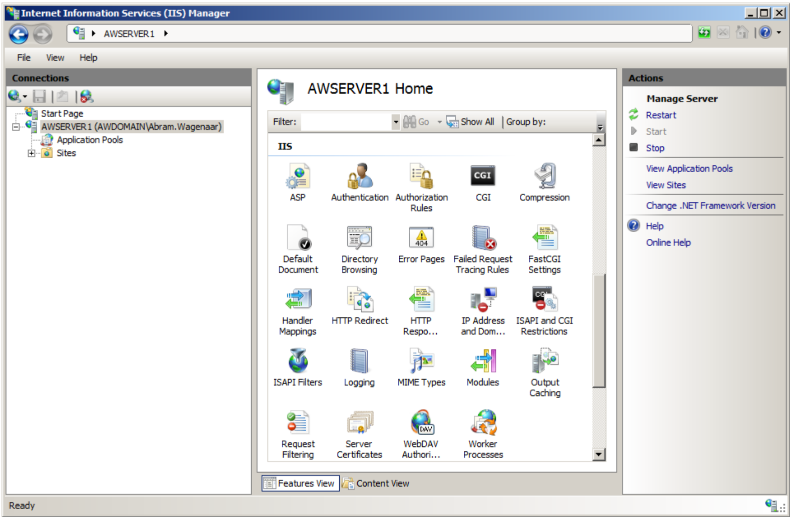
Windows XP / Windows Vista / Windows 7 / Windows 8 / Server 2003 / Server 2003 R2 / Server 2008 / Server 2008 R2 / Server 2012:

- 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

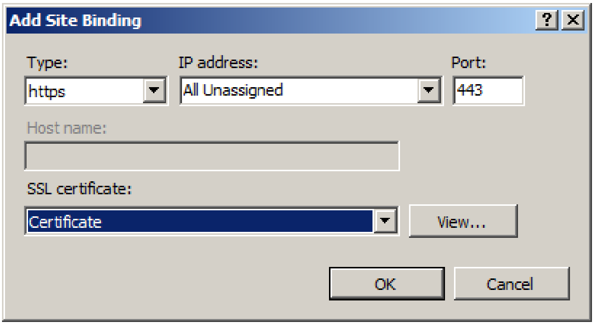
How do I enable an SSL Server Certificate in IIS 7 or 7.5?

To facilitate secure communication between clients and WebAdministrator/MobileAdministrator, it is recommended to enable an SSL Server Certificate in Internet Information Services (IIS).

To enable an SSL Server Certificate in IIS 7 and 7.5 (Windows Vista, Windows 7 and Windows Server 2008/R2), open **Internet Information Services (IIS) Manager**. Using Windows Server 2008, IIS Manager can be found under **Start** > **All Programs** > **Administrative Tools**. Alternatively, click **Start** > **Run** and enter the command *inetmgr*. This command also works for Windows 7 users.



Select your server in the **Connections** panel. In the middle of the screen, navigate to the **IIS** category and double click on **Server Certificates**. On the Actions panel, click **Create Self-Signed Certificate**. After entering a friendly name for the certificate, it will be created and listed in the Server Certificates panel. Note that the default expiration date of the certificate is exactly one year ahead of the date of creation.



Type: https

IP address: All Unassigned

Port: 443

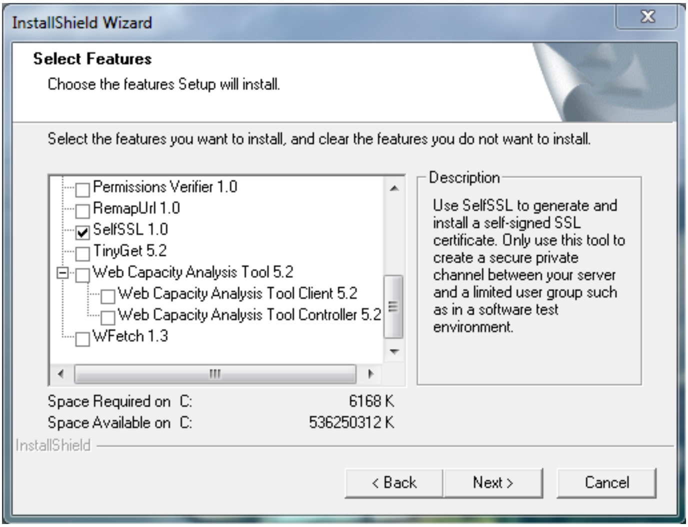
SSL certificate: Certificate

To apply the certificate to site communication, select the appropriate site in the **Connections** panel. On the **Actions** panel at the right, choose **Bindings**. Click **Add** to add a new binding. Select *https* as **type** and select the certificate you just added in the **SSL certificate** dropdown. Click **OK** to add the binding.

Accessing WebAdministrator and MobileAdministrator through a secure connection is now possible by replacing the *http://* prefix in your browser with *https://*, for example *https://servername/gdadmin*. Because of the self-signed certificate, your browser may issue a warning before allowing you to open WebAdministrator or MobileAdministrator. The communication, however, will still be fully encrypted.

How do I enable an SSL Server Certificate in IIS 5 or 6?

To facilitate secure communication between clients and WebAdministrator/MobileAdministrator, it is recommended to enable an SSL Server Certificate in Internet Information Services (IIS).



InstallShield Wizard

Select Features

Choose the features Setup will install.

Select the features you want to install, and clear the features you do not want to install.

- □ Permissions Verifier 1.0
- □ RemapUrl 1.0
- ☑ SelfSSL 1.0
- □ TinyGet 5.2
- □ Web Capacity Analysis Tool 5.2
  - □ Web Capacity Analysis Tool Client 5.2
  - □ Web Capacity Analysis Tool Controller 5.2
- □ WFetch 1.3

Description

Use SelfSSL to generate and install a self-signed SSL certificate. Only use this tool to create a secure private channel between your server and a limited user group such as in a software test environment.

Space Required on C: 6168 K

Space Available on C: 536250312 K

To enable an SSL Server Certificate in IIS 5 (Windows XP) or IIS 6 (Windows Server 2003), you can use the Microsoft tool SelfSSL, which is available in the IIS 6.0 Resource Kit Tools (a free download from the **Microsoft website**). By performing a **custom** setup, you can select the tools that you want to install. Select **SelfSSL 1.0**. After installation, open the SelfSSL command prompt through **Start** > **Programs** > **IIS Resources** > **SelfSSL**.

With a single command, you can assign a self-signed certificate to your website: *selfssl /N:CN=localhost /K:2048 /V:365 /S:1 /T*. Press **Enter**. Confirm the certificate creation by pressing **Y**. This will create a certificate for the default IIS site on the local server, and add localhost to the list of trusted certificates. The key length will be 2048 and the certificate will be valid for 365 days. If your site is not the default site of IIS, look up its Identifier in **Start** > **Administrative Tools** > **Internet Information Services (IIS) Manager** and change the parameter */S:1* accordingly.

Accessing WebAdministrator and MobileAdministrator through a secure connection is now possible by replacing the *http://* prefix in your browser with *https://*, for example *https://servername/gdadmin*. Because of the self-signed certificate, your browser may issue a warning before allowing you to open WebAdministrator or MobileAdministrator. The communication, however, will still be fully encrypted.

Index