G Data
Business
Software

User Manual

Table of contents

1. Introduction

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.

1.1. 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	★	★	★		★	★	★	★	★

1.2. 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

1.3. 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, 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**.

1.4. 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: www.gdata-software.com

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

2. 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.
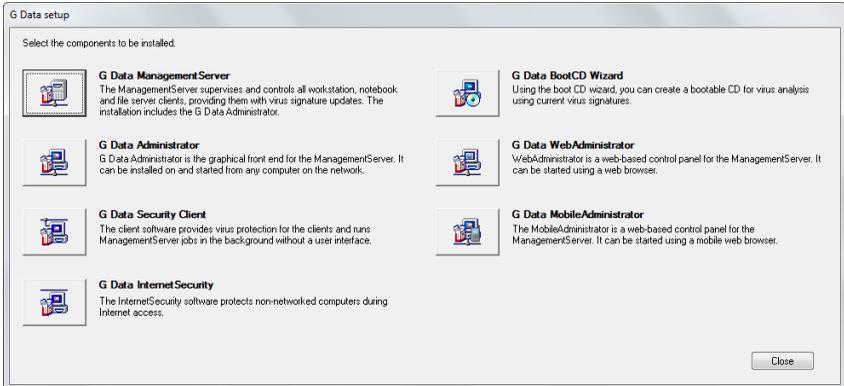
- **G Data ManagementServer**: Install this component first. G Data ManagementServer will be used to manage all G Data-related settings and updates. G Data ManagementServer lies at the core of the G Data architecture: it administers the clients, automatically requests the latest software and virus signature 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 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 boot CD.

- **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.

2.1. 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.

2.1.1. System requirements

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

Minimum system requirements

G Data ManagementServer/G Data MailSecurity MailGateway

- Operating system: Windows 8, Windows 7, Windows Vista, Windows XP SP3 (32-bits), Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, or Windows Server 2003
- RAM: 1 GB

G Data Administrator/G Data WebAdministrator/G Data MailSecurity Administrator

- Operating system: Windows 8, Windows 7, Windows Vista, Windows XP SP3 (32-bits), Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, or Windows Server 2003

G Data MobileAdministrator

- Operating system: Windows 8, Windows 7, Windows Server 2012, or Windows Server 2008 R2

G Data Security Client

- Operating system: Windows 8, Windows 7, Windows Vista, Windows XP SP3 (32-bits), Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, Windows Server 2003, or Linux kernel 2.6.25 or higher

G Data Internet Security for Android

- Operating system: Android 2.1 or higher
- Disk space: 14 MB

G Data MailSecurity for Exchange (64-bits Exchange plugin)

- Mail server: Microsoft Exchange Server 2013, Microsoft Exchange Server 2010, or Microsoft Exchange Server 2007 SP1

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

Recommended system requirements

When using G Data ManagementServer/G Data MailSecurity MailGateway with a local SQL database or other demanding applications on the same computer, the following recommended system requirements apply:

- RAM: 4 GB
- CPU: multicore

2.1.2. 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)

MailSecurity MailGateway server
- Port 7182 (TCP): Communication with G Data MailSecurity Administrator

MailSecurity Exchange plugin
- Port 7171 (TCP): Communication with G Data Administrator

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, after 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*.

2.1.3. G Data boot CD

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

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 boot CD you have created yourself**: To create your own G Data boot CD, 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 boot CD. Insert the CD into the drive.

2 Restart the computer. The G Data AntiVirus boot CD start menu will appear.

3 Use the arrow keys to choose the appropriate language, confirm your choice with **Enter**, and then choose **G Data AntiVirus**. A Linux operating system starts from the CD/DVD and the G Data AntiVirus boot CD interface appears.

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

4 If you have created a G Data boot CD yourself, the virus signatures are the latest ones that the G Data Security Client had available at the time the boot CD was created. If the virus signatures are outdated, the program will suggest updating them. Click **Yes** and perform the update. Make sure to enter your

registration number or, if you have already registered the G Data Software, your access credentials.

5 You will now see the program interface. Click **Computer** to check your computer for viruses and malware. Depending on the type of computer and size of the hard drive, the 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 have been restored.

7 After completion of the virus check, click the Close button (top right of the Linux program interface) then select **Exit** > **Shutdown**.

8 Remove the G Data boot CD 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.
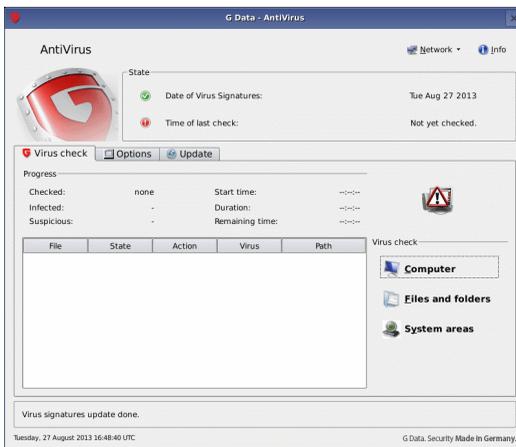

2.1.3.1. Create G Data boot CD

To create your own G Data boot CD, 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.
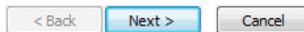
After finishing the installation, navigate to **Start** > **(All) Programs** > **G Data** > **G Data BootCD Wizard** and click **Create BootCD**. The wizard will lead you through the process of creating the G Data BootCD image. Make sure to let the wizard perform a virus signature update, in order to 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.

2.1.3.2. 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.

2.2. Installing G Data ManagementServer

Insert the G Data DVD and press the **Install** button, then select G Data ManagementServer. 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.

After choosing an installation folder, the server type can be chosen. 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, 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 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. An alternative is 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.

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. Next, 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 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. **Be sure to make a note of your user name and password and save them somewhere!** 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). 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 only occurs if you reinstall G Data ManagementServer or if a SQL database is already installed on the computer. Usually it is sufficient to close this message box by clicking on the **Close** button.

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 administer G Data ManagementServer, 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.

2.3. 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.

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**.

2.4. 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.

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. For more information about installing IIS, see the Reference Guide.

- **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.

2.5. 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.

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 Windows 7/Microsoft Windows Server 2008 R2**: MobileAdministrator requires at least Windows 7 or Windows Server 2008 R2.

- **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. For more information about installing IIS, see the Reference Guide.

- **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.

2.6. 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.

> When installing G Data Security Client on a server, make sure that it does not interfere with existing server workflows. For example, for database and e-mail servers, monitor and scan job exceptions should be defined for some files and folders. Consult the Reference Guide for more information.

2.6.1. 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:

- Gdmms.exe must be allowed network access (firewall exceptions need to be set).
- In a Windows Workgroup, Simple File Sharing (Windows XP) or the Use Sharing Wizard option (Windows Vista or Windows 7) must be disabled. It is enabled by default in all Windows client installations and can be disabled by opening any folder in Windows Explorer, clicking Organize > Folder and search options > View, and unchecking the option Use Sharing Wizard.
- User Account Control (UAC) must be disabled.
- Access permissions for the UNC shares C$ and Admin$ should be available. This can be a local or domain administrator account. An account password must be set: an empty password field is not permitted.
- The Remote Registry service must be enabled in Services.
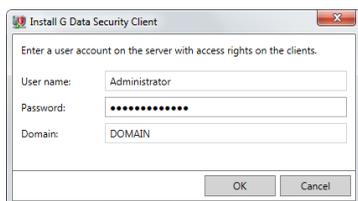
Using the **Server setup wizard**, which is automatically run the first time you start G Data Administrator, you get an overview of all enabled computers in the network. You can also manually add and enable computers by name. Alternatively, the Clients module allows you to install G Data Security Client 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. After initializing a remote installation, the **Installation overview** window is automatically opened. After a successful installation, the client needs to be rebooted.

> 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.

2.6.2. 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).

2.6.2.1. G Data Software DVD

Place the G Data DVD in the client computer's DVD drive and press the **Install** button, then select the G Data Security Client component.

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.

2.6.2.2. Install 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.

2.6.3. 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.

2.6.3.1. 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 Security 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. Installation progress will be shown in the **Installation overview** window.
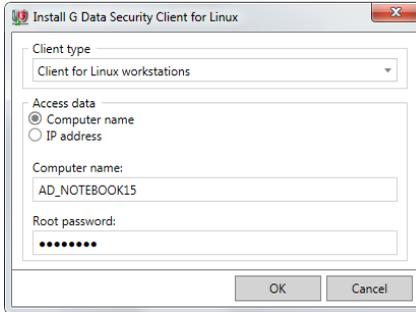
2.6.3.2. Local installation

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)

2.7. Installing G Data MailSecurity

G Data MailSecurity can be installed as a stand-alone gateway solution or as a plugin for Microsoft Exchange Server 2007 SP1/2010/2013. When installing the gateway solution, several configurations are possible, depending on the point in the network where it will be installed. The mail security gateway 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. 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 **Incoming (SMTP)** function in the **Options** window.

- 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 **Incoming (POP3)** function in the **Options** window.

- 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 **Outgoing (SMTP)** function in the **Options** window.

MailSecurity MailGateway can be installed on a dedicated server or on the mail server itself. Whichever case is chosen, several options (IP addresses, ports) should be configured directly after installing MailSecurity MailGateway. Example port configurations for various deployment scenarios can be found in the Reference Guide.

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. The installation 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 the gateway solution 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. 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**.

2.8. Installing G Data Internet Security for Android

To make use of G Data's Mobile Device Management capabilities, you can install a specially tailored business version of G Data Internet Security 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 Internet Security 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 **Mobile** > **Authentication for mobile clients**.

G Data mobile business client

A   to me
3 hours ago   Details

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://AWSERVER13:7184/gdata/mms/client/file/GD-MobSec-BUS.apk
Alternative link: http://10.202.3.42:7184/gdata/mms/client/file/GD-MobSec-BUS.apk

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

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

_____
Virus checked by G Data AntiVirus

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 Internet Security 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.

3. 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.

4. 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.
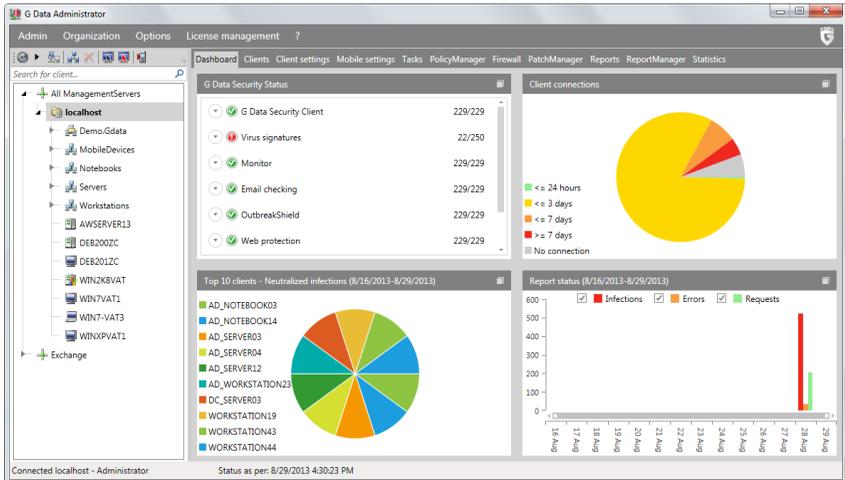
The Administrator interface is organized as follows: the client management area found on the left displays all clients which have been enabled, and to which G Data Client software can be or has already been deployed. To the right, all modules are accessible via dedicated tabs. The content of the module 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.

4.1. 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**.
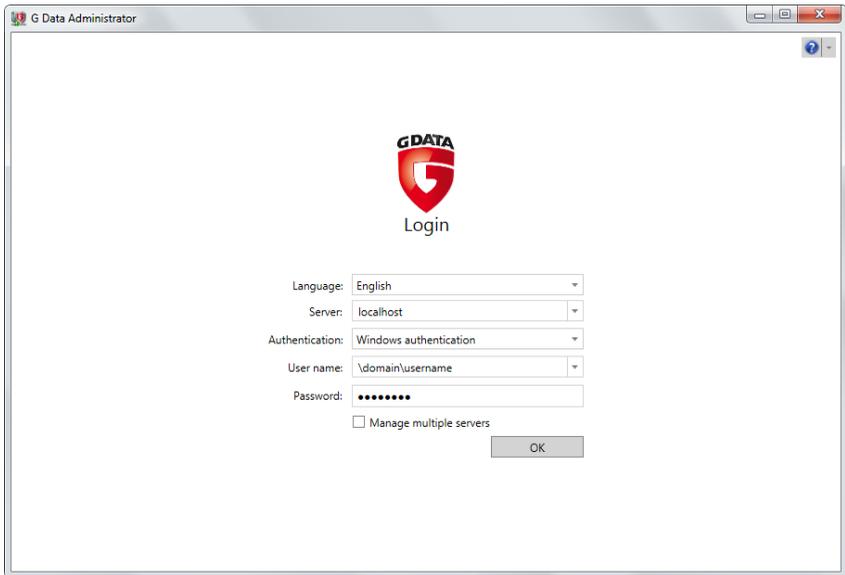
When starting G Data Administrator, you will be prompted for the **server**, **authentication**, **user name** and **password**. In the Server field, enter the name of the computer on which G Data ManagementServer was installed, then select your authentication type:

- **Windows authentication**: Log in using your Windows administrator 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**.

Click the arrow next to the question mark menu to reveal two additional options. **About G Data Administrator** shows version information. **Reset settings** allows you to reset all settings that Administrator has saved, such as display options.

4.2. Configuring G Data Administrator

Before any clients are configured, it is recommended to walk through the most important settings of G Data Administrator and G Data ManagementServer, and optimize them for the enterprise network. This includes administrative tasks such as the Server setup wizard and User account management, and server settings such as Alarms, Update configuration and Email settings.

4.2.1. Administrative tasks

The administrative tasks can be accessed through the **Admin** menu in G Data Administrator's menu bar. Most of the tasks should be carried out at least once, before any further configuration and deployment is carried out.

4.2.1.1. 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.
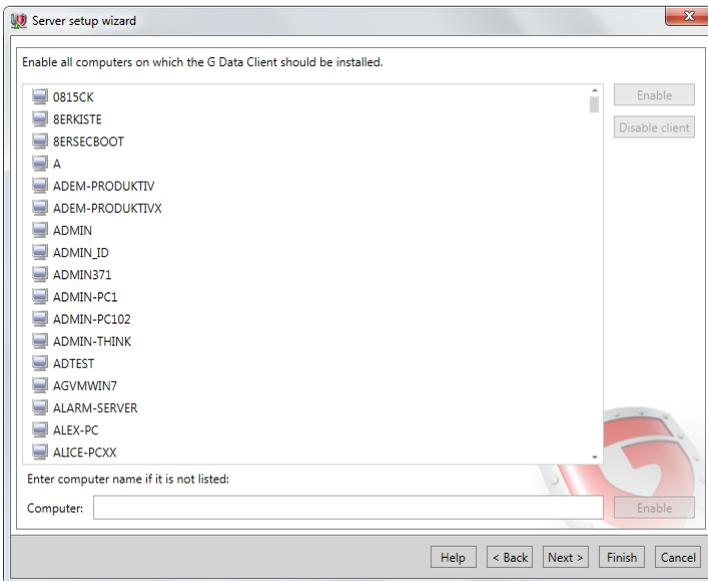
All clients that are to be managed by the G Data software must first be "enabled". To do this, highlight the clients to be enabled and click the **Enable** button. Some computers may not be included in the list (e.g. because the computers concerned have not been switched on for a long time or have not 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 will appear in the client list. When all computers to be protected have been enabled, click on **Next** to move on to the next step. If you have enabled any clients, in the next step 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.

G Data ManagementServer downloads new virus signatures and program files over the Internet. To automate the update process, entering the access data created during the online registration is required. A detailed description of update interval settings can be found in the section **Internet update**. Alternatively, access data and update intervals can be configured afterwards using the Internet update window.

Click **Next** to configure e-mail notifications. 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.

To enable mobile device management, some basic settings have to be configured. In the next step, enter a password with which mobile devices will have to authenticate with the ManagementServer. To be able to use emergency actions, you have to enter the **Sender ID** and **API key** of your Google Cloud Messaging account. For more information about Google Cloud Messaging accounts or to change the mobile settings afterwards, see **Server settings** > **Mobile**.

Click **Finish** to close the wizard. 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.

4.2.1.2. Display log

The log file offers an overview of the latest server- and client-side 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 actions.
- **Client/group**: Specify whether you would like to view a log for all clients, a group, 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 entries can be exported as an XML file, printed or deleted.
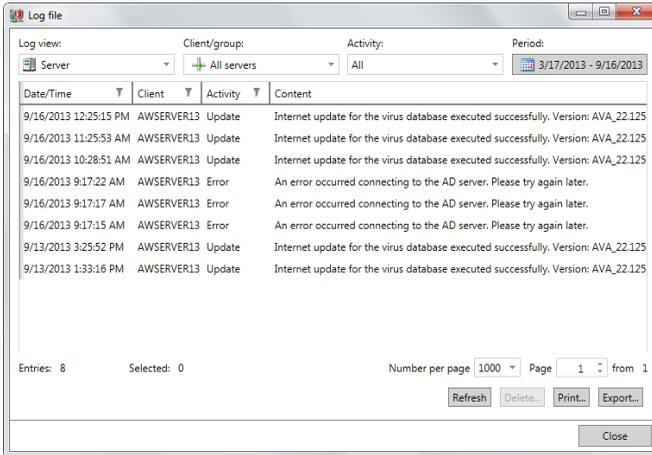
4.2.1.3. User account management

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.
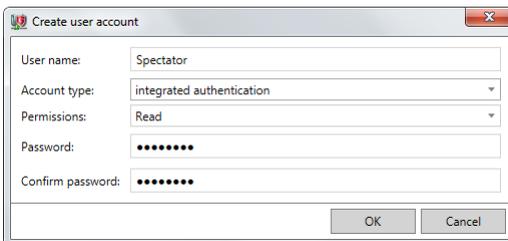
4.2.1.4. Manage server(s)

Using the Manage Server(s) 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. The allocation of clients or groups to subnet servers functions separately from the grouping of clients in the client management area. That means that clients that have been assigned to different subnet servers can still be grouped together.

- **Delete**: Remove a subnet server from the list. This does not remove the actual software from the subnet server.
- **Assign clients**: Assign existing clients to subnet servers.

- **Add subnet server**: Add a new subnet server. In the following dialog window, enter the **Computer name** of the prospective subnet server. Next, enter a user account with administrator permissions on the subnet server. Confirm with **OK** to initiate the remote installation, which can be tracked using the **Installation overview** window.

- **Uninstall server**: Initialize a remote deinstallation of the selected subnet server.

- **Authorize server**: To prevent unauthorized access to server data, locally installed subnet servers need to be authorized. Only after authorization will the ManagementServer start synchronizing data with the subnet server.

> Subnet servers that are installed remotely using the function **Add subnet server** are automatically authorized. Only locally installed subnet servers and subnet servers that have been upgraded to version 13 need to be authorized manually. A remote deinstallation can only be carried out on authorized subnet servers.

4.2.1.5. Synchronize subnet server(s) now

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

4.2.1.6. Exit

This function closes G Data Administrator. G Data ManagementServer will keep running in the background to carry out its tasks.

4.2.2. Options

In the menu bar, the Options menu offers access to settings mostly related to ManagementServer's functioning. Some of the options are configured when you run the **Server setup wizard** (such as **Internet update**), others should be configured manually.

4.2.2.1. Internet update

The Internet update function ensures that current virus signatures and the latest program files are always available. During the update procedure, the current virus definitions are downloaded from the G Data UpdateServer and saved on the G Data ManagementServer. The Internet update window lets you configure this process. Subsequent distribution of the virus signatures to the clients is managed through the **Clients** module.

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 update server are downloaded to the G Data ManagementServer. In the second step, the new files are distributed to the clients (see **Client settings** > **General**).
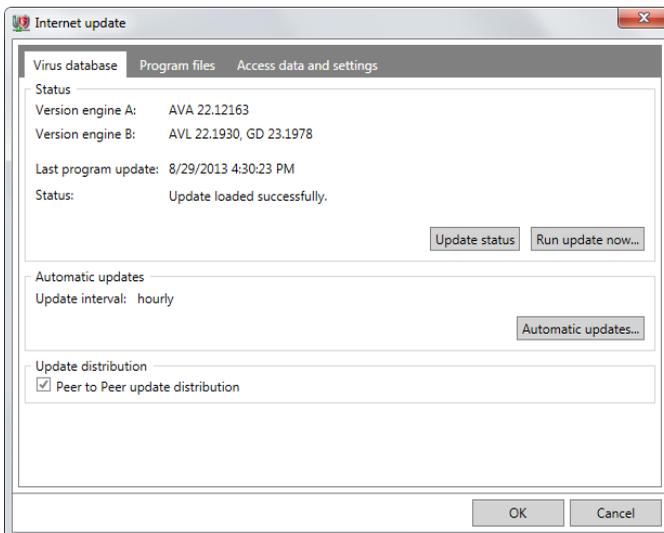
- **Update status**: Check the status of the virus signature update.
- **Run update now**: Carry out an immediate update of the virus database. The current virus signatures are downloaded to be distributed to the clients afterwards.

- **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 update server. In the second step, the new files are distributed to the clients (see **Client settings** > **General**).
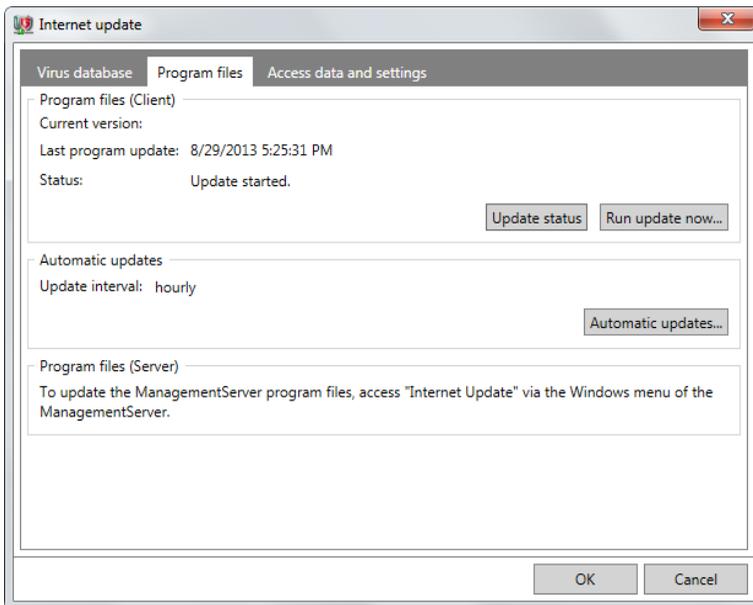
- **Update status**: Check the status of program file update.

- **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**: Configure Internet updates to be run automatically. Check **Run update periodically** and specify when 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 access data for updating the virus databases and program files. Enter these under **User name** and **Password**. Select the nearest **Region** to ensure optimal speed when downloading updates. The **version check** (enabled by default) should always be switched on because it improves update speed. If, however, problems arise with virus databases, switch off the version check. During the next update, the integrity of all virus database files will be checked and files will be redownloaded if necessary.

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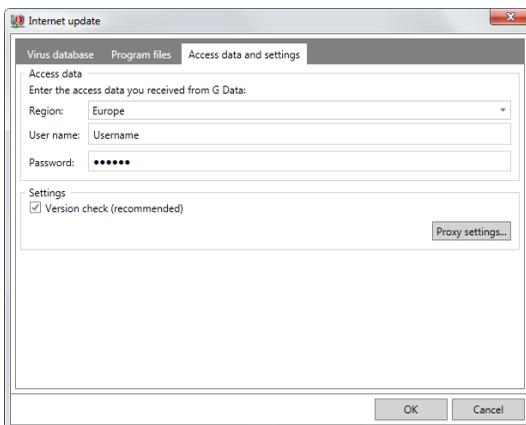
G Data software can use the Internet Explorer proxy connection data (from version 4). First configure Internet Explorer and check whether the test page of our update server is accessible: *http://ieupdate.gdata.de/test.htm*. In the **Proxy settings** window, switch off the option **Use proxy server**.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

4.2.2.2. 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 results**, **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. With recipient selected, click **Trigger test alarm** to send a test alarm.
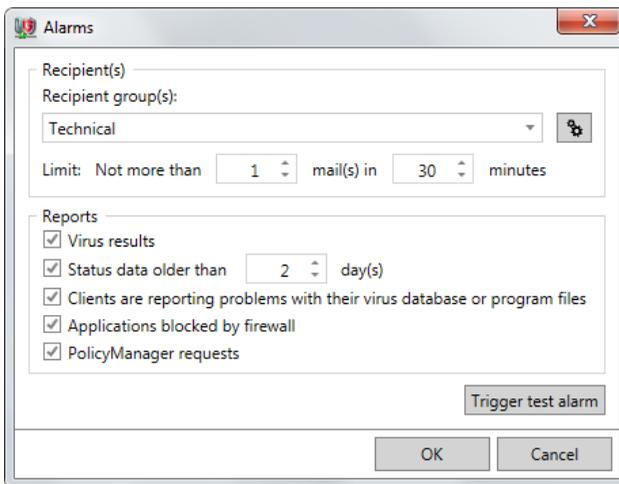
Click the cogs icon ( ) to open the **Email settings** window and define recipient groups.

4.2.2.3. Update rollback

In rare cases, a virus signature update can lead to a false alarm or similar problems. It can make sense to block the latest virus signature update and use a previous one instead. G Data ManagementServer saves the last few updates for each antivirus engine. Should the latest update for one of the engines result in problems, the network administrator can block it 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**. By default, the last five signature states are saved.
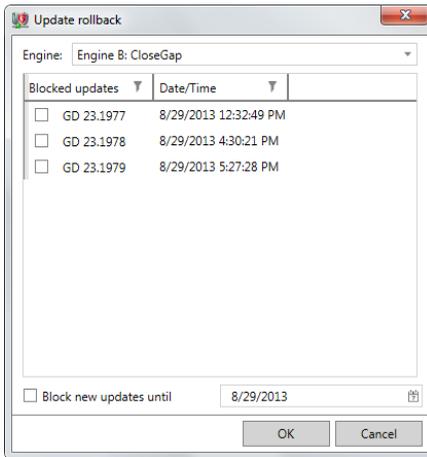
On clients that are not connected to G Data ManagementServer (e.g. notebooks used in business travel), no rollbacks can be carried out. A block of new updates from the server to the client cannot be retracted without contacting G Data ManagementServer.

With the affected engine selected in the **Engine** dropdown list, its most recent engine updates are listed under **Blocked updates**. Select the update(s) that should be blocked and click OK. Those updates will no longer be distributed, and clients that have previously received them will be rolled back to the most recent non-blocked update (when they connect to the ManagementServer). Optionally, new updates can be included in the block: tick **Block new updates until** and select a date.

4.2.2.4. Server settings

The Server settings window bundles configuration settings for ManagementServer functionalities such as synchronization, email settings, load limits, and staged software updates.

Settings

Under **Rollbacks** you can 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.
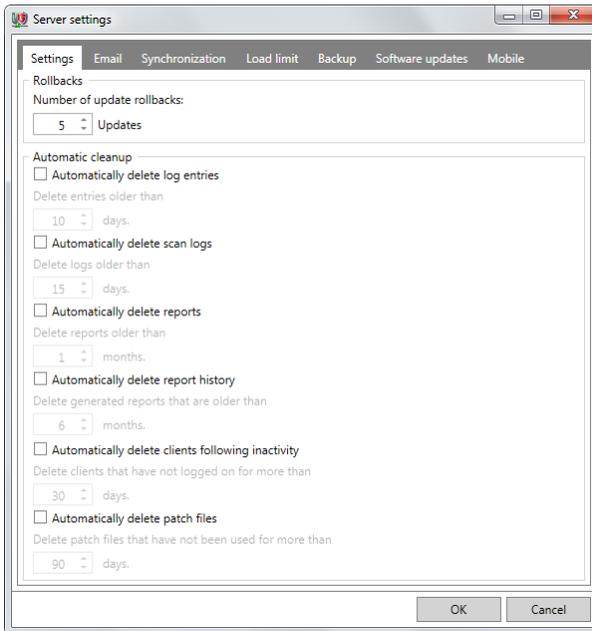
Automatic cleanup allows you to configure whether various items should automatically be deleted after a specified period of time.

- o **Automatically delete log entries**: Delete log files that are older than the set amount of days.

- o **Automatically delete scan logs**: Delete scan log files that are older than the set amount of days.

- o **Automatically delete reports**: Delete reports that are older than the set amount of months.

- o **Automatically delete report history**: Delete generated ReportManager reports that are older than the set amount of months.

- o **Automatically delete clients following inactivity**: Delete clients that have not logged on for a set amount of days.

- o **Automatically delete patch files**: Delete patch files that have not been used for more than the set amount of days.

Email

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. If your SMTP server requires authentication, click **SMTP authentication** to configure it. You can set up **SMTP AUTH** to authenticate directly on the SMTP server, or **SMTP after POP3**, if the SMTP server requires it.

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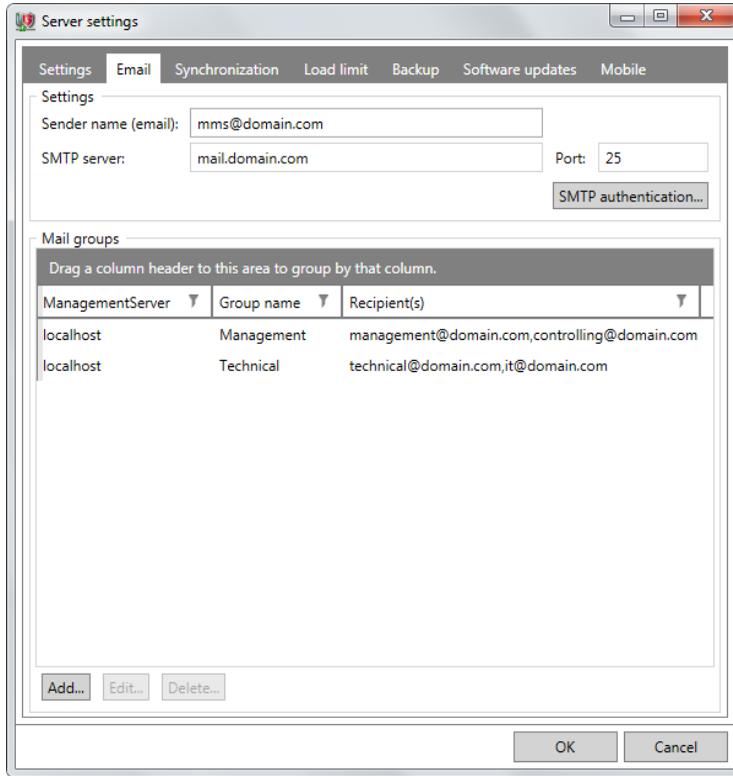
Synchronization

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 connect to the MMS to check for new updates or settings. 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**, 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. If you select a daily interval, you can define the exact time of the day at which the synchronization should take place. Active Directory synchronization is only carried out if at least one group has been assigned

an Active Directory Organizational Unit.
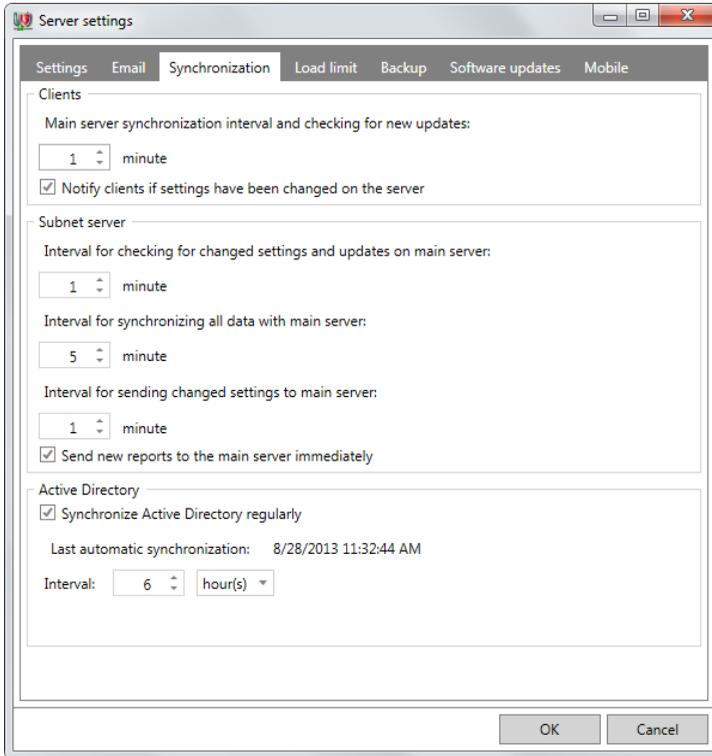
Load limit

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.
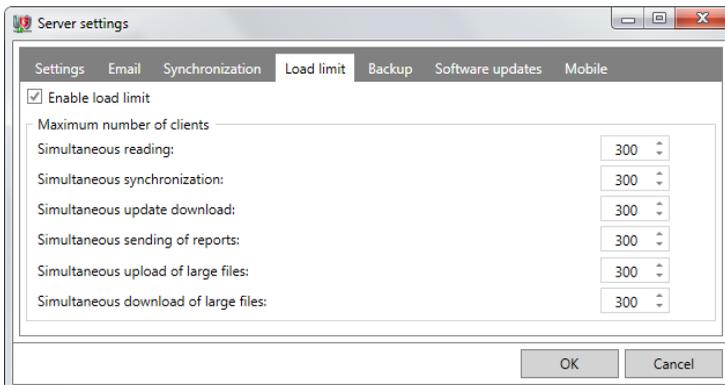
Backup

To make sure that backups are carried out successfully, enough free disk space needs to be available on the client (backup cache) and on the server (backup storage). For server and clients you can define threshold values for warning messages and error messages. When the amount of free disk space on the client or the server drops below the warning threshold, a warning message will be added to the Reports module, and the client cache will be automatically cleaned up, retaining the latest archive but removing all others (if they have been uploaded to the ManagementServer). When the amount of free disk space on the client or the server drops below the error threshold, an error message will be added to the Reports module. Server backup storage and client cache will be automatically cleaned up. If there is still not enough free disk space on the server, backups will not be carried out.

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.
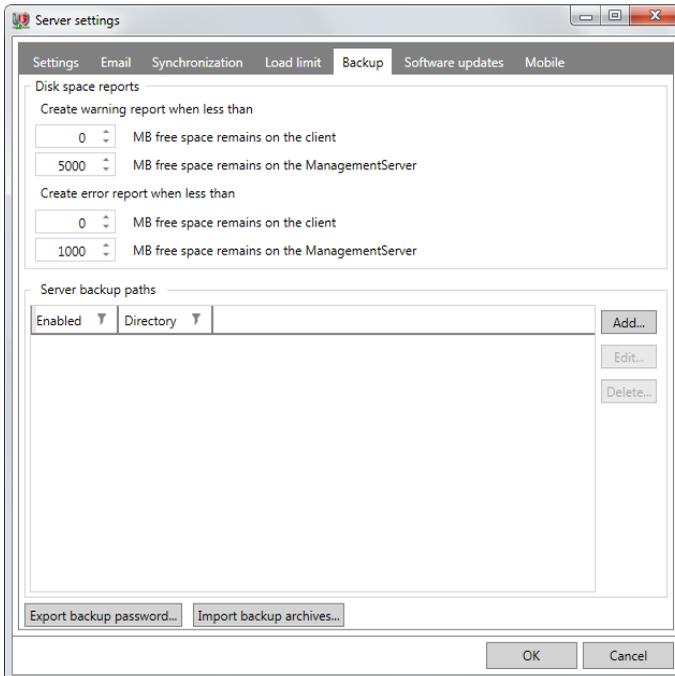
Software updates

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.
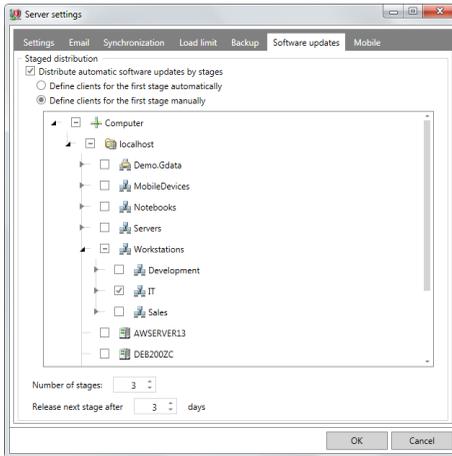
When you enable staged distribution, you can choose to have the clients for the first group be defined automatically, or manually pick the clients that should be the first to receive software updates. You can also choose the total number of groups and the delay between distribution among the different groups.

Mobile

The tab Mobile features some general settings for mobile device management. If they have not been configured using the Server setup wizard, authentication for mobile clients and Google Cloud Messaging should be configured here.

Under **Authentication for mobile clients**, enter a password with which mobile devices will have to authenticate with the ManagementServer. To be able to use emergency actions, you have to enter the **Sender ID** and **API key** of your Google Cloud Messaging account. Free accounts for this push notification framework can be registered at code.google.com/apis/console. Consult the Reference Guide for more information about registering a Google Cloud Messaging account.
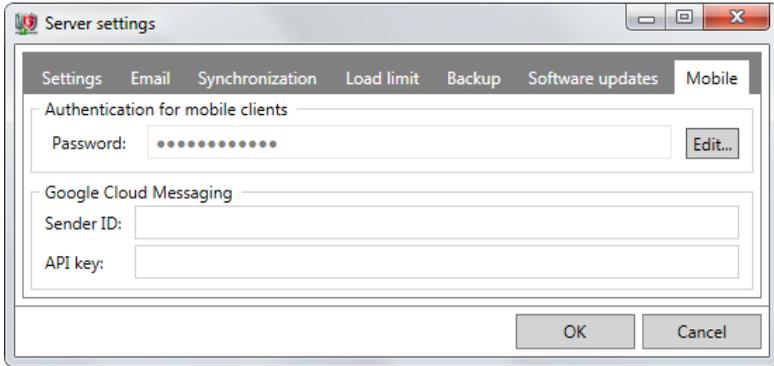
4.2.3. License management

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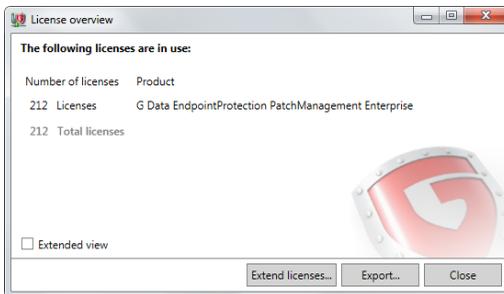
Using the button **Export** you can export the overview to a text file. By selecting **Extended view**, you get specific information about the servers on which the licenses are being used.

4.2.4. Help

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

4.3. Managing clients

Before clients can be managed using G Data Administrator, they need to be added to its client management area and enabled. There are several ways to add and enable clients, depending on network size and configuration. For smaller networks, adding clients through the **Server setup wizard** will suffice. For larger networks, the process can be streamlined and (partly) automated by using the **Find computer(s)** dialog

window or the built-in Active Directory support.
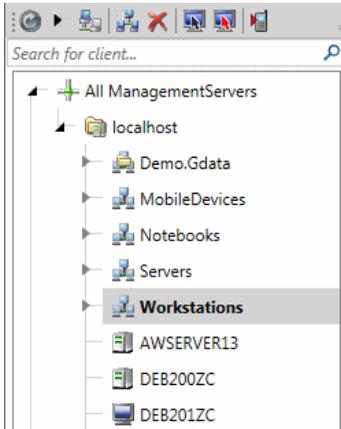
All enabled clients, servers, and groups in the network are listed in the client management area. As in Windows Explorer, groups that have subdivisions appear with a small plus symbol. If you click on them, the directory structure expands and enables the view of the structure below it. Clicking the minus symbol collapses the list. Depending on the type of node 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.

Using the client management area, you can import and export settings for single clients and for groups. Right-click on a client or group and choose Export settings to export settings from the **Client settings** and **PolicyManager** modules to a .dbdat file. To import settings, choose Import settings and select the scope and settings file.

Different client types are indicated by different icons, such as a ManagementServer, a group, an Active Directory Group, a desktop client, or a mobile client. The following types of icons are shown in the client management area:

Network

Server

Subnet server

Group

Group (Active Directory link)

Client

Linux client

Laptop client

Mobile client

Linux server

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

In the toolbar, you will see the most important client management commands, some of which are also displayed in the **Organization** menu:

Refresh

Expand/collapse all: Expand or collapse all items in the network tree.

Show disabled clients

Create new group

Delete

Enable client: To enable a computer, highlight it in the list and click the Enable button.

Installation overview

Send installation link to mobile clients: To deploy mobile clients from within G Data Administrator, send them an installation link to the G Data Internet Security app. This initiates the installation procedure for G Data Internet Security for Android.

4.3.1. Active Directory

G Data Administrator's Active Directory support imports computer objects from local domains' organizational units. Create a new group, right click it, and select the option **Assign AD item to group**. In the dialog window that opens, click **Assign to AD group** and select the LDAP server. The **Select...** button will provide 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** will initiate a remote installation of G Data Security Client for every computer that is added to the Active Directory domain, as long as it meets the remote installation requirements.

By default, G Data ManagementServer compares its data status to Active Directory every six hours. This value can be changed under **Server settings** > **Synchronization**.

4.3.2. Organization

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

4.3.2.1. Refresh

The Refresh function updates the client list in the client management area.

4.3.2.2. Show disabled clients

Using the option Show disabled clients, clients that have not (yet) been enabled can be shown. Disabled clients are shown as greyed out icons.

  Client (enabled)

  Client (disabled)

4.3.2.3. Create new group

Clients can be combined into groups to apply settings to multiple clients at once. Easily distinguishable security zones can be defined since all settings can be made for both single clients and for entire groups. Select a server or group, and then click the Create new group button. After entering a group name, clients can be assigned to the new group by dragging and dropping the desired client onto it.
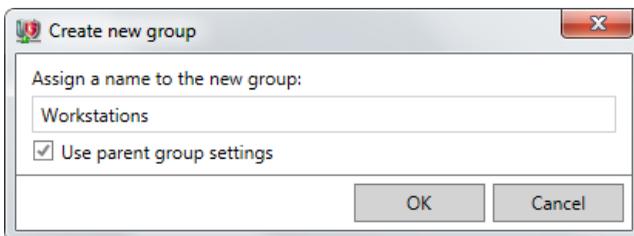
4.3.2.4. Edit group

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.
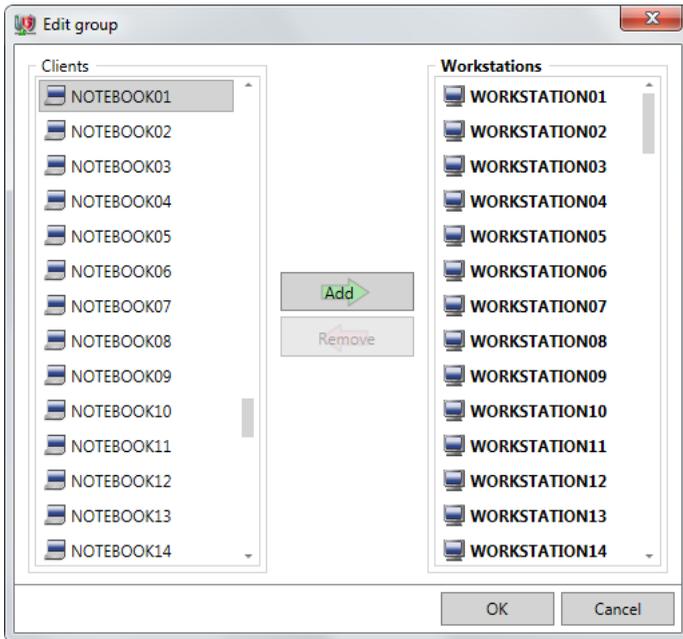
4.3.2.5. Delete

Individual clients can be removed from the client list with the Delete command. G Data Security 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.

4.3.2.6. Find computer(s)

The Find computer(s) window can be used to add network clients to G Data Administrator's client management area and enable them. Clients can be found by IP address and enabled directly from within the dialog window.

The Search computer window will contact all computers in a specified IP range. The range can be defined using a **Start IP** and **End IP** (such as 192.168.0.1 and 192.168.0.255), or a **Subnet address** (in CIDR notation, such as 192.168.0.0/24). To make sure that only available clients are listed, select **Only search for available clients (Ping)**. Click **Start search** to start the network search. Computers will be listed as soon as they are found. If the search process is taking too long, it can be canceled by clicking **Cancel search**.
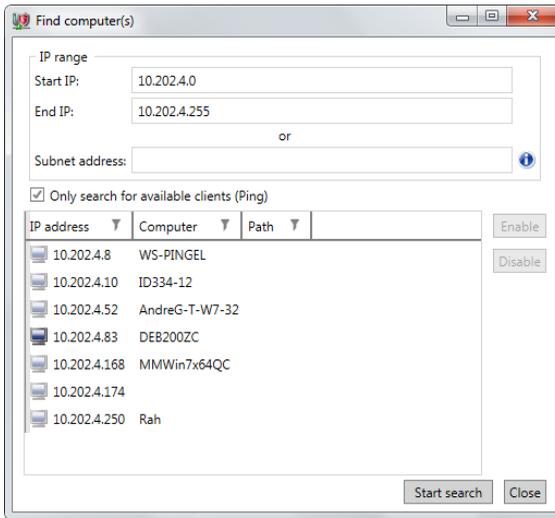
All computers that respond to the IP check are listed, including their IP address and computer name. Using the **Enable** button, the respective clients can be added to the client management area. The search result includes enabled clients, if applicable - these can be disabled by clicking **Disable**.

4.3.2.7. 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.

4.3.3. Installation overview

To keep track of the progress of the installation, the Installation overview window can be used. It opens automatically when a remote installation task is added, or can be opened by clicking the Installation overview button in the client management area's toolbar.
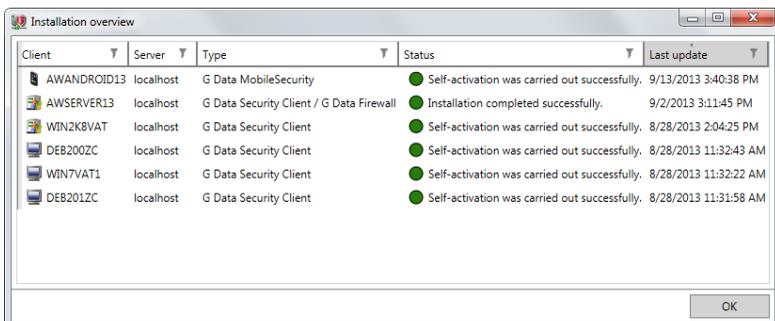
The Installation overview window lists all clients that have pending and completed remote installation tasks. The **Type** column shows the type of installation (G Data Security Client and/or G Data Firewall, or Subnet server). After a remote installation has been completed, the **Status** column will be updated. In most cases, the client will need to be rebooted in order to complete the installation: the installation procedure will add a report to the **Reports** module if a reboot is required.

4.4. 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	▼	Last access	▼
▼ **G Data Security Client version:** (21)								
▼ **G Data Security Client version:** 12.0.0.222 (11.01.2013) (1)								
▼ **G Data Security Client version:** 12.0.0.239 (11.04.2013) (28)								
▼ **G Data Security Client version:** 13.0.0.13 (29.08.2013) (1)								
▲ **G Data Security Client version:** 13.0.0.7 (25.08.2013) (197)								
▼ **Last access:** (11)								
▼ **Last access:** 8/21/2013 1:53:53 PM (5)								
▼ **Last access:** 8/25/2013 1:53:53 PM (6)								
▲ **Last access:** 8/26/2013 1:48:01 PM (7)								
	AD_NOTEBOOK14		AVA 22.12133 (28.08.2013)		AVL 22.1928 (28.08.2013		8/26/2013 1:48:01 PM	
	AD_NOTEBOOK15		AVA 22.12133 (28.08.2013)		AVL 22.1928 (28.08.2013		8/26/2013 1:48:01 PM	
	AD_NOTEBOOK16		AVA 22.12133 (28.08.2013)		AVL 22.1928 (28.08.2013		8/26/2013 1:48:01 PM	
	AD_NOTEBOOK17		AVA 22.12133 (28.08.2013)		AVL 22.1928 (28.08.2013		8/26/2013 1:48:01 PM	

Changed client settings are only saved once the **Apply** button has been clicked. Click the **Discard** button to use 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. At the bottom of most modules, the **Information** status field shows whether the settings have been successfully transferred to the clients.

4.4.1. Dashboard

The Dashboard module shows information about the current status of the clients in the network.
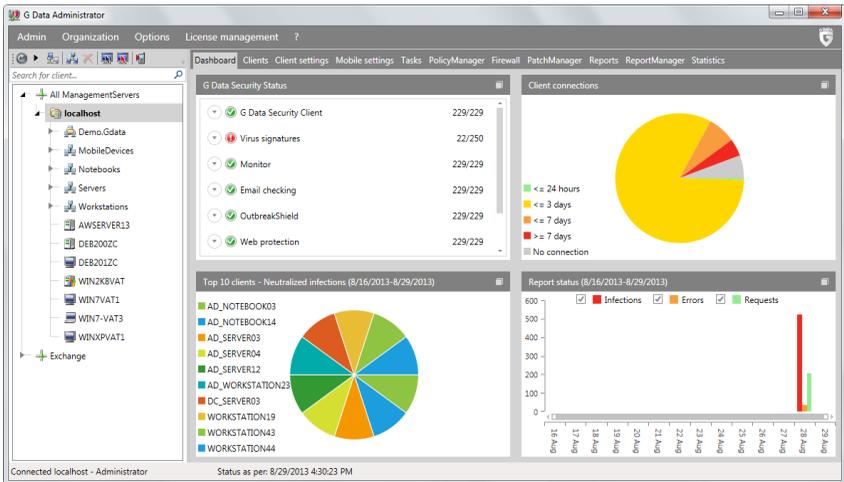
G Data Security Status shows all the basic security settings for the clients or groups that you have highlighted in the client management area and immediately deploy changes if necessary.

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.

The **Client connections** chart offers an overview 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. The clients that appear under **Top 10 clients - Neutralized infections** 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** offers visual representation of the number of infections, queries, and errors in your network during a configurable time period.

4.4.2. Clients

The Clients module offers you client management functions, such as information about whether the clients are running normally and if the virus signatures and program files are fully up to date.

4.4.2.1. Overview

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

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**
- **Security status**
- **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**
- **EULA**

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.

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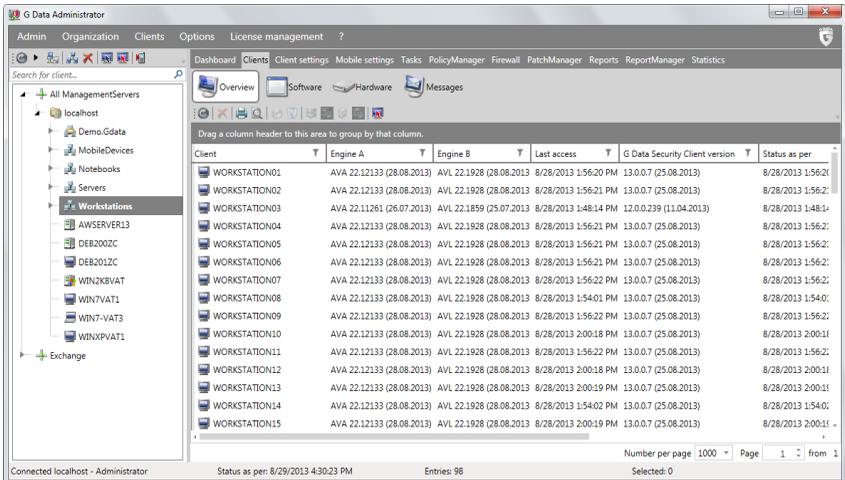
When the Overview panel is selected, an additional menu entry named Clients becomes available in the menu bar. It reflects the options that are also available by right-clicking one or more clients. The following options are included:

- **Install G Data Security Client**
- **Install G Data Security Client for Linux**
- **Uninstall G Data Security Client**
- **Installation overview**
- **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.
- **Edit assigned EULA**: Assigns a previously defined **EULA** to the selected client(s) (only available for mobile clients).
- **Remove assigned EULA**: Removes an assigned EULA from the selected client(s) (only available for mobile clients).
- **EULA management**
- **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 the uninstall function, G Data Security Client can be remotely removed. Before the uninstallation procedure is initiated, you can select the components that should be kept. It is possible to uninstall the client software while keeping the jobs, reports, messages or backup archives that are associated with that client and have been saved on the server. Select the components to be removed and click **OK** to initiate the uninstallation. For a complete removal the client must be restarted.
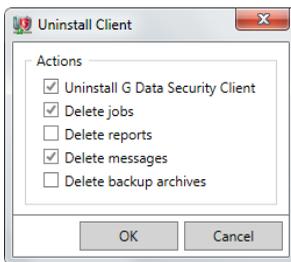

Alternatively it is also possible to uninstall the client locally. This requires a command prompt with administrator rights. In the C:\Program Files (x86)\G DATA\AVKClient directory, enter the command *unclient /AVKUninst* to start the uninstallation. The computer should be restarted afterwards.

Manage EULAs

The Manage EULAs window allows you to add, edit and remove End User License Agreements (EULAs) for mobile devices. Using the appropriate options in the Clients menu, these EULAs can then be assigned to any mobile device to make sure the end

user is informed about and has agreed with the deployment of G Data's Internet Security app.
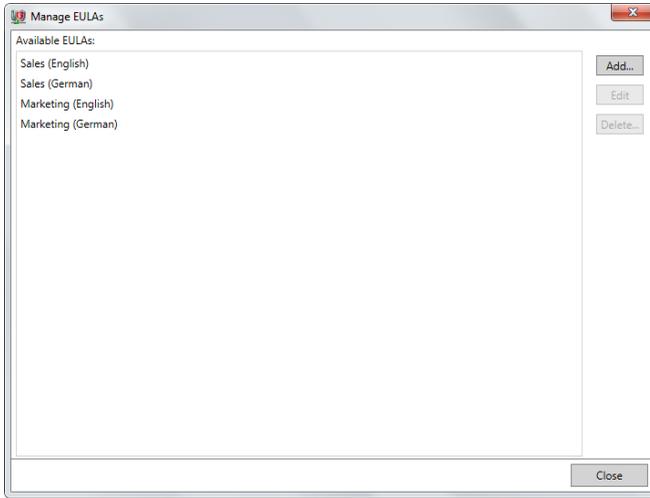
The Edit EULAs window lists all available EULAs. To add an EULA, click **Add**. In the Create EULA window, enter a **Name**, select a **Language** and add the **Content** of the agreement. Clicking **OK** adds the EULA to the list.

To edit an existing EULA, select it in the list and click **Edit**. To remove an EULA, select it and click **Delete**.

4.4.2.2. Software

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.

The software overview can be managed with the following toolbar buttons:

Refresh: Refresh the software overview.

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

Print: Print the software 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.

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.

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.

4.4.2.3. Hardware

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

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

- **Client**
- **CPU**
- **CPU speed (MHz)**
- **Internal memory**
- **Free system storage space**
- **System storage space (statistics)**
- **Free storage space**
- **Total storage space (statistics)**
- **System vendor**
- **System name**
- **System version**
- **System family**
- **CPU ID**
- **Mainboard vendor**
- **Mainboard**
- **Mainboard version**

- **Bios vendor**
- **Bios release date**
- **Bios version**

The hardware overview can be managed with the following toolbar buttons:

Refresh: Refresh the hardware overview.

Print: Print the hardware 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.

4.4.2.4. 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.
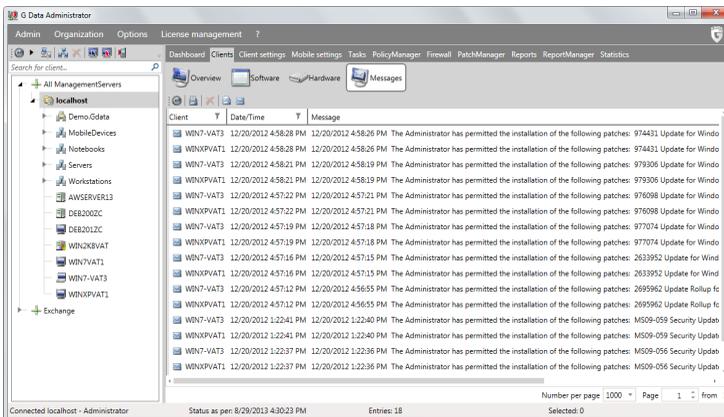
To create a message, simply click the **New** button. In the dialogue, you can select the clients you want to send the message to. If you want a message to be accessible only to certain users of a client computer or network, enter their login names under **User name**. Type your information in the **Message** field and click the **Send** button.

4.4.3. 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.

4.4.3.1. General

The General tab allows you to set general settings for the selected clients.
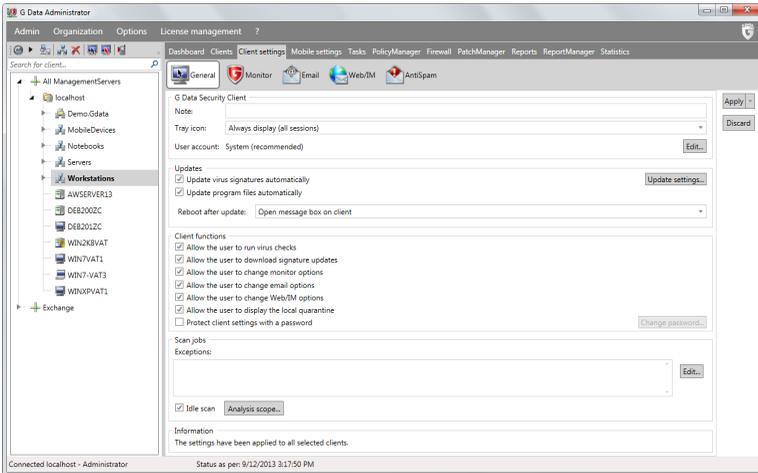
G Data Security Client

The G Data Security Client section covers basic client functionality.

- **Note**: Enter any notes or remarks that apply to this client.

- **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

The Updates section lets you define virus signature and program file update settings.

- **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 to download virus signatures directly from the ManagementServer; clients will then check for updates every **synchronization interval**. Alternatively, you can grant them the right to obtain updates from the G Data update servers. For mobile workstations, mixed mode is recommended: 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 signature updates for the latter two options.

Client functions

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

- **Allow the user to 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. Additionally, this lets users change settings for local virus checks.

- **Allow the user to download 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.

- **Allow the user to change monitor options**: If this function is enabled, the client user has the option to change the **Monitor** settings.

- **Allow the user to change email options**: If this function is enabled, the client user has the option to change the **Email** and **AntiSpam** settings.

- **Allow the user to change Web/IM options**: If this function is enabled, the client user has the option to change the **Web/IM** settings.

- **Allow the user to display the 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 client settings 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.

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

> 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.

4.4.3.2. Monitor

The Monitor panel allows you to configure the most important aspects of client protection. 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.
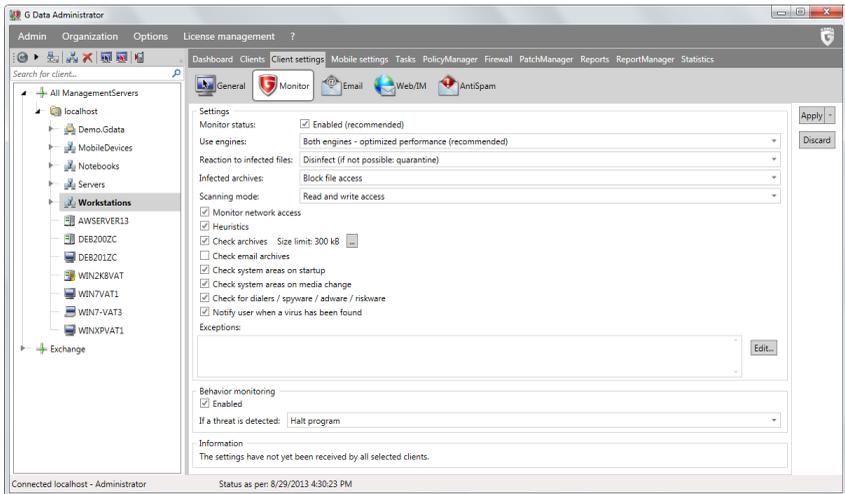
Settings

Monitor settings can be used to configure its scans and define exceptions.

- **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:

  o **Block file access**: Neither read nor write access will be granted for an infected file.

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

  o **Disinfect (if not possible: quarantine)**: An attempt is made to remove the virus; if this is not possible, the file is moved to Quarantine.

  o **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.

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

  o **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.

- **Check 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.

Under **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 complete path and filename of the process (e.g. *C:\Windows\system32\cmd.exe*).

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**.

4.4.3.3. 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.
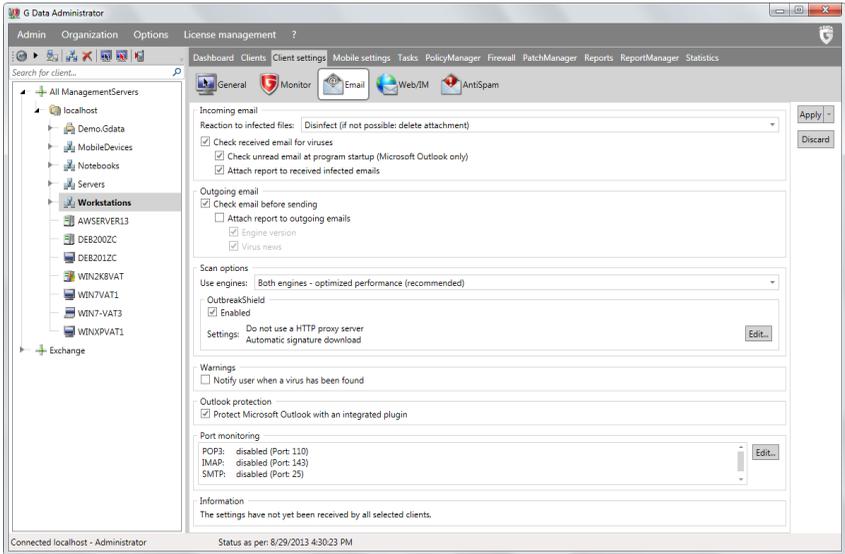
Incoming email

The Incoming email section defines options for scanning incoming emails.

- **Reaction to infected files**: 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 startup (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

The Outgoing email section defines options for scanning outgoing emails.

- **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

The Scan options section configures the scan parameters for incoming and outgoing emails.

- **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 **Edit**, 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

The Warnings section configures warning messages for recipients of infected emails.

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

Outlook protection

Outlook protection enables email scans using an integrated plugin.

- **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.

4.4.3.4. 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.
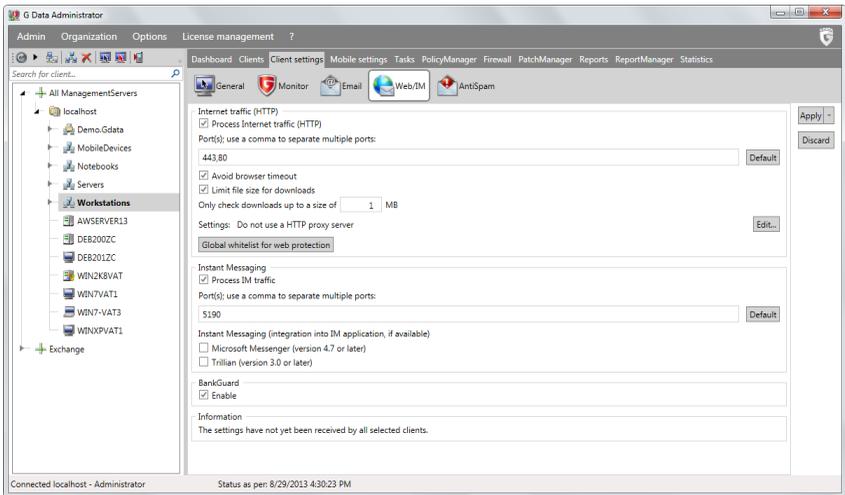
Internet traffic (HTTP)

The section Internet traffic (HTTP) covers scan settings for HTTP traffic.

- **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 internet traffic check.

Instant Messaging

The section Instant Messaging covers scan settings for instant messaging traffic.

- **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, Firefox, and/or Chrome.

4.4.3.5. 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.
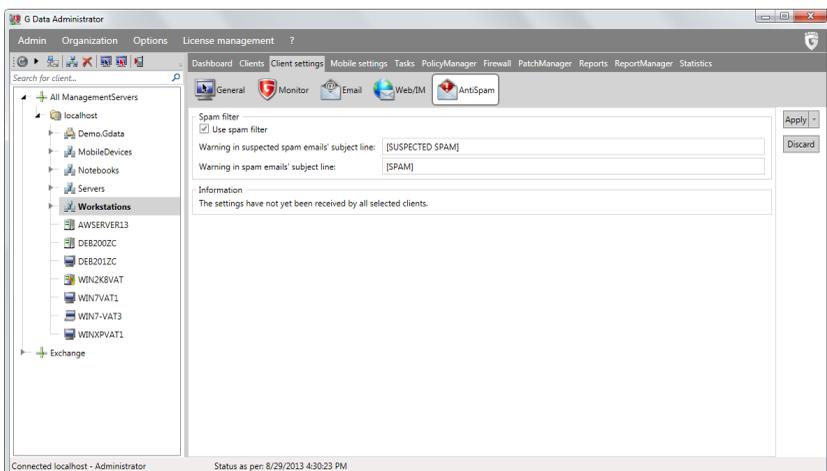
> You or the user can define a rule in the client's email software to automatically move mail that has *[Spam]* in the subject line to a special folder for spam and junk mail.

4.4.4. Mobile settings

The Mobile settings tab offers easy access to G Data Administrator's mobile device management capabilities. After having deployed G Data Internet Security to one or more Android devices, they will show up in the client management area. Selecting a mobile client or group contains mobile clients offers access to its settings on the Mobile settings tab.

4.4.4.1. General

The General tab offers settings for automatic updates, web protection, virus checks and synchronization, as well as two general device management options.

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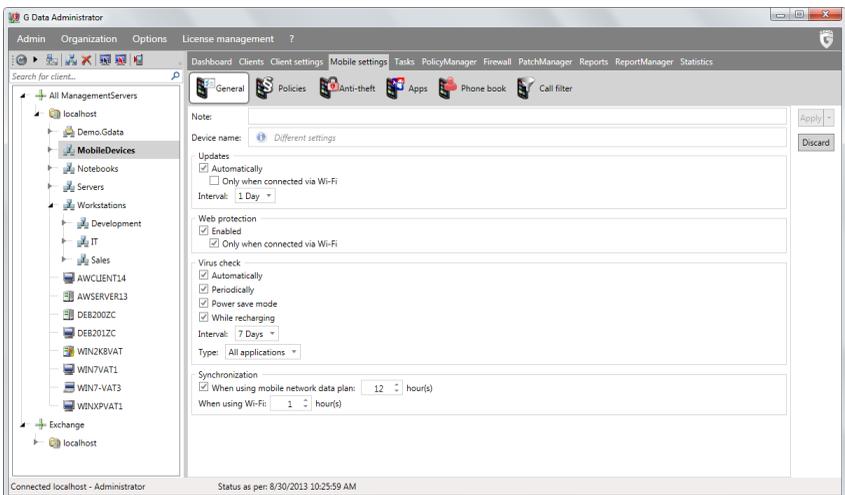
Updates

The Updates section covers settings related to updates.

- **Automatically**: You can configure whether the mobile client should automatically check for software and virus signatures. If updates are not downloaded automatically, the user can still initiate a manual update. 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

The Web protection section includes the possibility to limit web protection to WLAN networks.

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

Virus check

The Virus check section lets you define parameters for on-demand and on-access virus scans.

- **Automatically**: Enable an automatic virus check for newly installed applications.
- **Periodically**: Enable a periodic virus check. Tick the checkbox Periodically and specify the **Interval**.
- **Power save mode**: Postpone the periodic virus check if the device is in power save mode.
- **While recharging**: Run the periodic virus check only when the device is being charged.
- **Type**: Scan **all applications** or only **installed applications**.

Synchronization

The Synchronization option defines how often the mobile client synchronizes its data with the ManagementServer. You can set an interval and configure synchronization to happen only when there is Wi-Fi connectivity or also when using a mobile network data plan.

4.4.4.2. Policies

By assigning each mobile device a phone type, you can enforce policies. This allows you to block certain device functions from being used on corporate devices and to protect the corporate network.
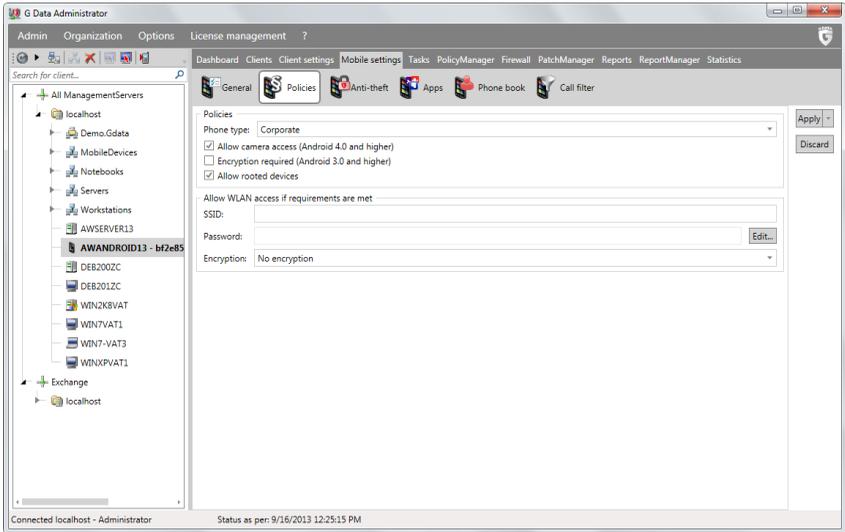
Policies

Under Policies, select the **Phone type** that the selected device(s) belong to. For devices that have been issued by the company, select Corporate. This will lock down various settings of the mobile app so that the end user cannot inadvertently change them. Regardless of the phone type, some functions can be blocked or enforced:

- **Allow camera access**: allow access to the device's camera (Android 4.0 and higher)
- **Encryption required**: require full device encryption to be enabled (Android 3.0 and higher)
- **Allow rooted devices**: allow devices that have been rooted. If disabled, rooted devices are blocked using the remote maintenance password defined under **Anti-theft**. If disabled, rooted devices cannot access the WLAN defined under **Allow WLAN access**.

Allow WLAN access

For devices that have been rooted, access to a specific WLAN network can be blocked. This allows you to permit access to the corporate WLAN network only for devices that can be securely managed.

Enter the **SSID** for the corporate network for which access should be enabled. Select the **Encryption** and enter the **Password** (if the network is encrypted).

4.4.4.3. Anti-theft

The Anti-theft tab offers a range of functions that help protect devices and their data if they go missing. Devices that are stolen or lost can be remotely locked, wiped, located or muted by sending an SMS from a trusted phone number. Using Google Cloud

Messaging, these anti-theft functions can also be triggered manually at any time.

Before specifying any anti-theft measures, some general settings should be entered. The **Remote maintenance password** consists of numbers and functions as a PIN code. When sending SMS commands to the device, the password has to be included to ensure that only authorized users can send commands. The command to remotely reset the maintenance password can only be sent from the **Trusted phone number**. Some commands trigger a report or other notification. Enter an **Email address for notifications** to which these messages will be sent.
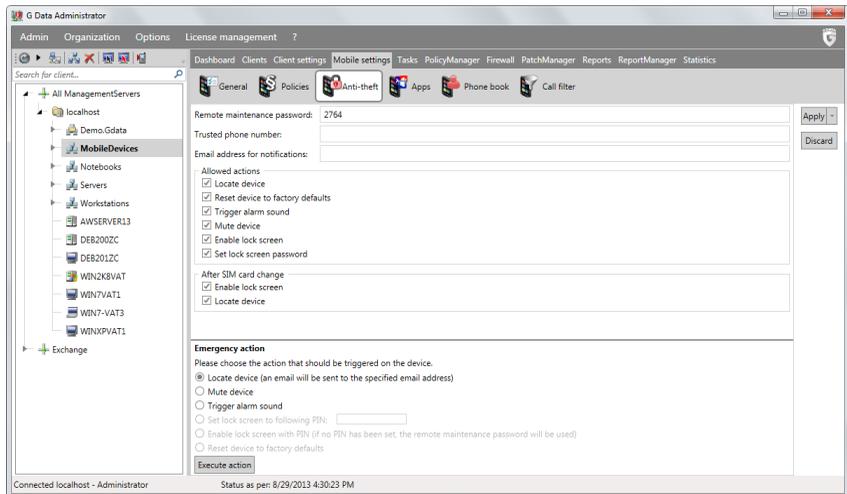
Allowed actions

Under Allowed actions, you can define anti-theft actions that can be triggered by SMS. These actions can be trigged by sending the respective command to the device, including the remote maintenance password.

- **Locate device**: The device will send its location to the email address specified for notifications. To activate this feature via SMS, send an SMS containing the text *password* **locate**.

- **Reset device to factory defaults**: The device will be reset to its factory settings. All personal data will be wiped. To activate this feature via SMS, send an SMS containing the text *password* **wipe**.

- **Trigger alarm sound**: The device will play a ringtone until Internet Security is started. This will assist in locating lost devices. To activate this feature via SMS, send an SMS containing the text *password* **ring**.

- **Mute device**: 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 via SMS, send an SMS containing the text *password* **mute**.

- **Enable lock screen**: The device screen can be locked to prevent the device from being used. To activate this feature via SMS, send an SMS containing the text *password* **lock**. If no lock screen password has been set, the remote maintenance password will be used.

- **Set lock screen password**: Set a password to unlock the device if the lock screen feature has been enabled. To activate this feature via SMS, 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.

To remotely reset the remote maintenance password, send an SMS from the phone number that you specified under **Trusted phone number** containing the text **remote password reset:** *newpassword*.

After SIM card change

When deploying Internet Security for Android, it remembers which SIM card is in the device at that time. If this card is changed at any time, for example if the device was stolen and resold, certain actions can be carried out automatically.

- **Enable lock screen**: same functionality as the option under **Allowed actions**.
- **Locate device**: same functionality as the option under **Allowed actions**.

Emergency action

Using the internet-based Google Cloud Messaging, an emergency action can be triggered on a device. This has the advantage of working even if the device is being used without a SIM card. Google Cloud Messaging needs to be configured first: enter **Sender ID** and **API key** under **Server settings** > **Mobile**. Select any of the following actions and click Execute action to send the command to the device immediately:

- **Locate device**: same functionality as the option under **Allowed actions**.
- **Mute device**: same functionality as the option under **Allowed actions**.
- **Trigger alarm sound**: same functionality as the option under **Allowed actions**.
- **Set lock screen to following PIN**: same functionality as the option under **Allowed actions**.
- **Enable lock screen with PIN**: same functionality as the option under **Allowed actions**.
- **Reset device to factory defaults**: same functionality as the option under **Allowed actions**.

4.4.4.4. Apps

The Apps panel lets you configure access to apps on managed devices. To block or allow apps, first decide whether the filter should work in Blacklist or Whitelist **Mode**. In Blacklist mode, all apps on the blacklist will be blocked or password protected; all others will be accessible. In Whitelist mode, all apps on the list will be allowed or password protected; all others will be blocked. The **Password** (a PIN code) is used to access blocked apps. You can also choose to enter a **Recovery email address** to which the password will be sent in case you forget it.
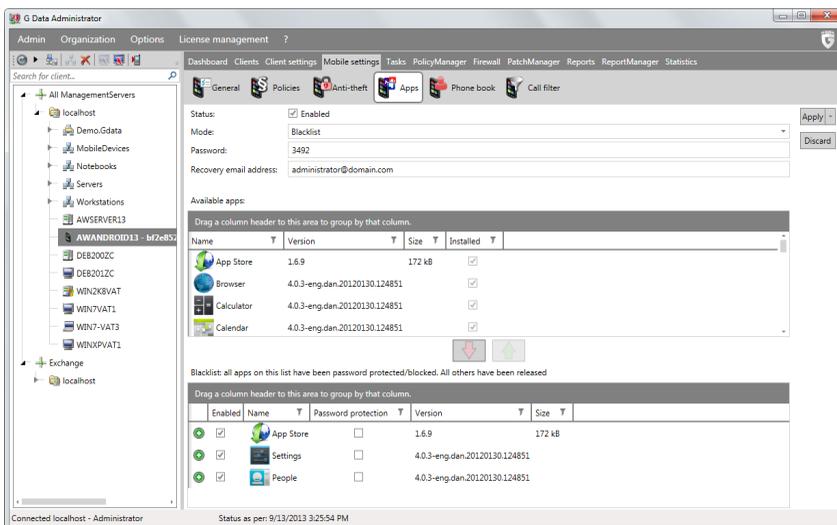
Under Available apps, all apps that have been installed on the currently selected device (s) are listed. For each app, you can see its **Name**, **Version**, **Size** and **Installed** date. Using the arrow controls apps can be moved to the white-/blacklist. For apps on the white-/blacklist, you can enabled or disable **Password protection**.

4.4.4.5. Phone book

The Phone book panel allows for advanced contacts management. Contacts can be added to a phone book within the Internet Security app and they can be hidden from the device's built-in phone book. In combination with the **Apps** feature, the Phone book can be configured as a centrally managed replacement for the Android phone book, creating a managed contacts environment for scenarios where the communication possibilities of a mobile device should be limited to a pre-approved subset of contacts.

The main list shows all contacts that have been added to Internet Security's phone book. For each contact, the **First name**, **Last name**, **Phone number**(s) and **Address** are listed. Using the **Visibility** dropdown menu, you can decide whether the contact should be **Visible** in the Android phone book, **Hidden** from the Android phone book, or if its calls and SMS messages should be hidden (**Communication hidden**).
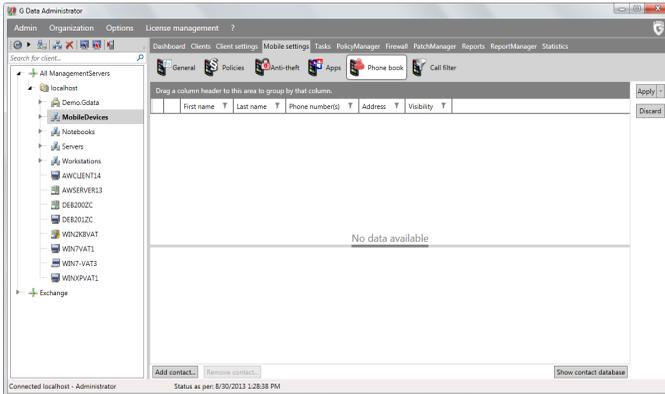

To add a contact to the phone book, click **Add contact**. The **Contact database** window will show all contacts that have been defined. Select one or more contacts and click **Choose** to add the contacts to the phone book. To remove a contact from the phone book, click **Remove contact**.

To add a contact to the contact database, click the button **Create contact** in the toolbar or **Import contacts** to import contacts from an Active Directory Organizational Unit (OU). When creating a contact, you should at least enter a **First name** or **Last name**. Additionally, one or more addresses can be added, as well as e-mail addresses, phone numbers, fax numbers, and organizations. To remove a contact from the contact database, select it and click the **Delete** icon in the toolbar or the option **Delete** in the context menu.

4.4.4.6. Call filter

The Call filter allows you to filter incoming calls and SMS messages as well as outgoing calls. Using the same contact database as the **Phone book** panel, you can easily add contacts to a blacklist or whitelist, as well as defining general filters.
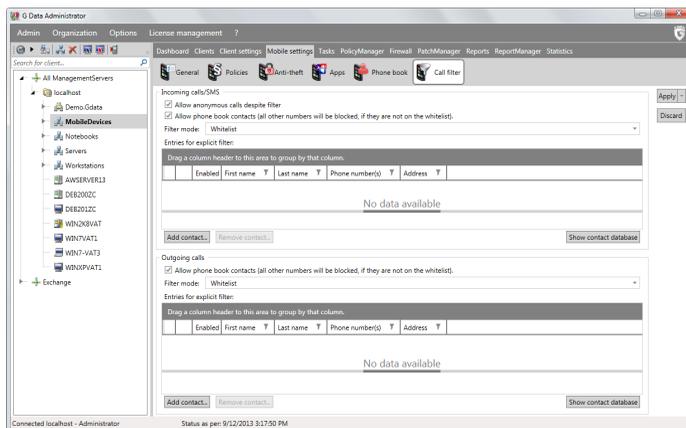
Incoming calls/SMS

Under Incoming calls/SMS, you can define how Internet Security should treat incoming communication. Uncheck **Allow anonymous calls despite filter** to block all anonymous incoming calls. Checking **Allow phone book contacts** will always allow contacts with an entry in the device phone book through the filter.

Under **Filter mode**, you can define specific measures for incoming calls and SMS messages. Select **Blacklist** to allow all communication, except from the contacts that are on the list. Select **Whitelist** to block all communication, except from the contacts that are on the list. By clicking **Add contact**, you can add any contact from the contact database to the list. Click **Remove contact** to remove a contact from the list.

Outgoing calls

Under Outgoing calls, you can define how Internet Security should treat outgoing phone calls. Checking **Allow phone book contacts** will always allow contacts with an entry in the device phone book to be contacted.

Under **Filter mode**, you can define specific measures for outgoing calls. Select **Blacklist** to allow all communication, except from the contacts that are on the list. Select **Whitelist** to block all communication, except from the contacts that are on the list. By clicking **Add contact**, you can add any contact from the contact database to the list. Click **Remove contact** to remove a contact from the list.

If an attempt is made to call a blocked contact, the user will be informed and offered the possibility to request the contact to be released. This will add a report to the **Reports** module using which the administrator can directly add a blacklist or whitelist release for the contact.

4.4.5. Tasks

In the Tasks module, you can define tasks, or jobs, for the 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.
- **Client**: 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 execution**: When the respective job was last run.
- **Interval**: This column shows the cycle with which the job will be repeated according to the defined schedule.
- **Scope**: Find out which media (e.g. local hard disks) the analysis includes.
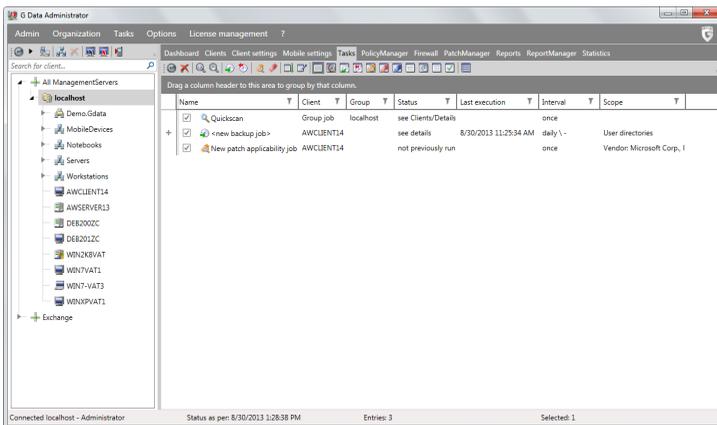
To manage tasks, you can use the following options from the toolbar above the task list:

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 job: This function allows you to restore backups to clients or groups. For more information about backup jobs, see the chapter Restore jobs. The Restore function is only available as part of the Enterprise solutions.

Patch applicability job: List software and patches that have been installed on clients or groups. For more information about software recognition jobs, see the chapter Patch applicability jobs. The Patch applicability 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.

All jobs

Only scan jobs

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

Only recovery jobs (only available as part of the Enterprise solutions)

Only patch applicability jobs (only available as part of the optional PatchManagement module)

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

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

Only single scan jobs

Only periodic scan jobs

Only pending scan jobs

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.

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 specific types of jobs. 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.
- **Restore backup**: Restore backups to clients or groups. For more information about backup jobs, see the chapter Restore jobs. The Restore function is only available as part of the Enterprise solutions.
- **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).

4.4.5.1. Scan jobs

The Scan job window lets administrators define a single or periodic scan job. A complete job configuration consists of three aspects: **Job scheduling**, **Scanner** settings and **Analysis scope**, each covered by their respective window tabs.

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. Enable **Report scan progress to the ManagementServer** to report the status of a scan process to the server every two minutes.

Permissions can be granted to the users for pausing or aborting the job via the system tray context menu. **Shut down client after scan job, if no user is logged on** 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**.
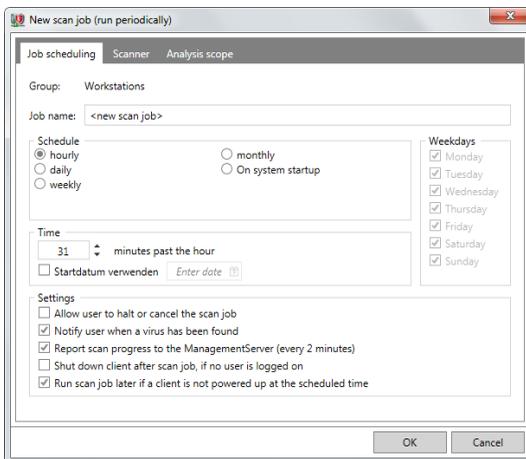

For periodic scan jobs, this tab also specifies when and at what intervals the virus check should occur. If you select **On system startup** the scheduling defaults no longer apply and the G Data software will run the scan each time your computer is restarted. For **Daily** jobs, you can specify under **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 - optimized performance**. 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. These settings are identical to those found on the panel **Client settings** > **Monitor**.

- **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. Most of the settings are identical to those found on the panel **Client settings** > **Monitor**, but the following ones are specific to scan jobs:

  - **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).
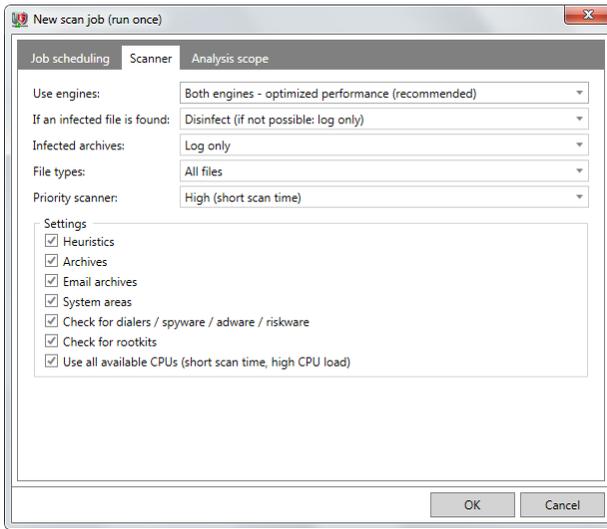
Analysis scope

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.
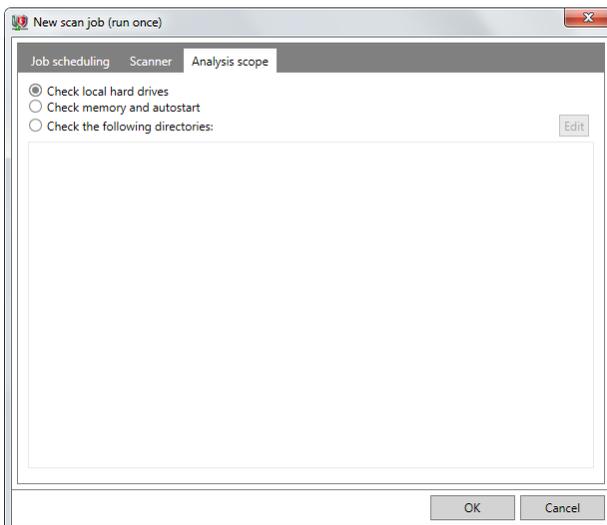
4.4.5.2. Backup jobs

The Backup function is available as part of the Enterprise and SmallBusiness Security solutions. It lets administrators plan backup tasks for client data, to centrally secure essential files.

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 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 running on battery** 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 under **Server settings** > **Backup**, 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.

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.
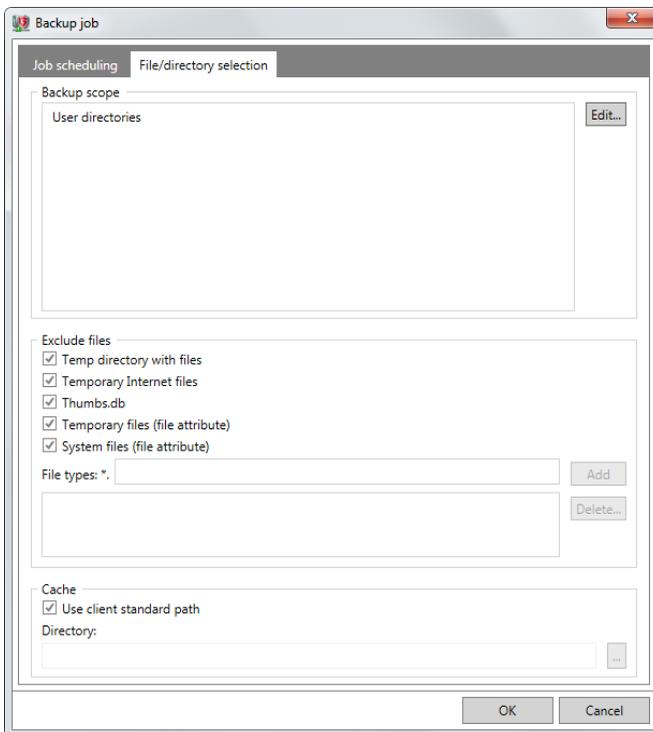
4.4.5.3. Restore jobs

Restore jobs can be planned in several ways. In the **Tasks** menu, select **New** > **Restore job** to plan a new restore job. The **Restore job** toolbar button opens the same window, allowing you to select a backup to restore. Alternatively, you can look up the backup in the list of backup jobs. Right click a job and click **Restore backup** to open the **Restore backup** window.
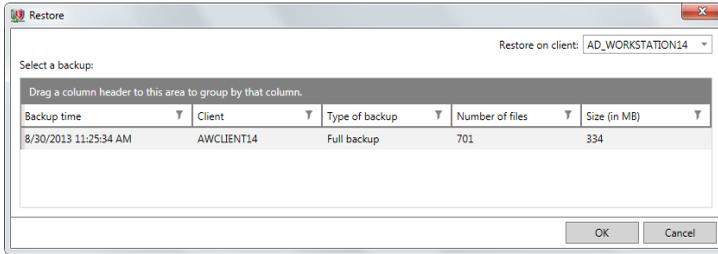
The Restore backup window shows some basic information about the selected backup job. It contains one or more backups, depending on how often the job was run. Per backup, the list shows **Backup time**, **Client**, **Type of backup**, **Number of files** and **Size (in MB)**. In the **Restore on client** dropdown, you can select the client to which the backup should be restored (this does not need to be the client on which the backup was made). Select the appropriate backup and click **OK** to open the **Restore settings** window.

The restore settings can be configured on two tabs. **File selection** allows you to browse through the backup. Click **Only restore selected files from the archive** to enable the folder tree in which you can select the files to be restored. Click **Restore all files within the archive** to disable the folder tree and restore all files instead. The **Options** tab lets you configure restore job settings. You can add a descriptive title to the restore job under **Job name**. Files can be restored to the directory they were backed up from if you select **Restore files to original directory**, or to another directory if you select one under **Target directory**. Finally, you can decide what should happen to file conflicts under **Overwrite existing files**. Upon confirming the recovery settings, a restore job will be added to the Tasks module. It will be carried out immediately.

4.4.5.4. Patch applicability jobs

The Patch applicability function is available as part of the optional PatchManagement module.

Patch applicability jobs can be planned to check clients or groups for applicable patches. The applicability 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 scan for. To add a specific attribute (Vendor, 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.
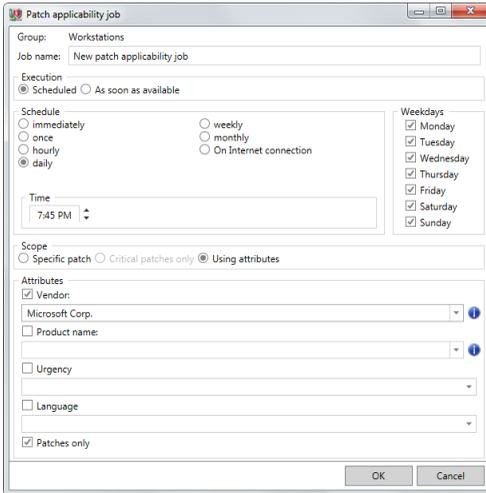
4.4.5.5. Software distribution jobs

The Software distribution function is available as part of the optional PatchManagement module.
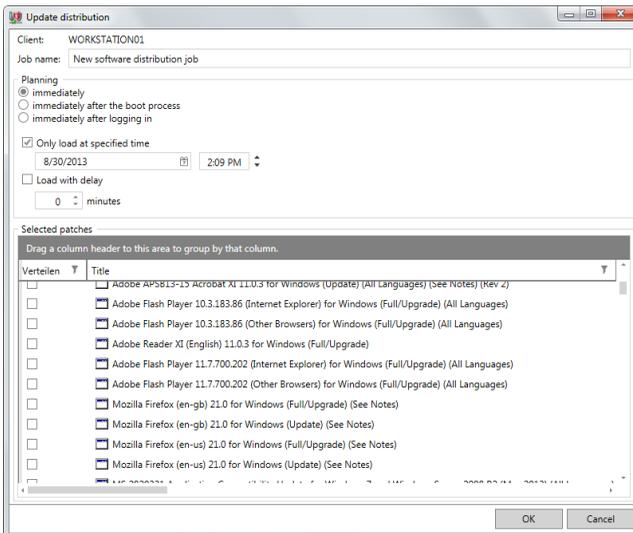
To distribute applicable patches to clients or groups, you can define a software distribution job. By ticking the option **Only load at a specified time**, you can schedule the job. The actual software distribution can be carried out **immediately**, **immediately after the boot process**, or **immediately 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**.

4.4.6. PolicyManager

The PolicyManager module is 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.

4.4.6.1. 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.
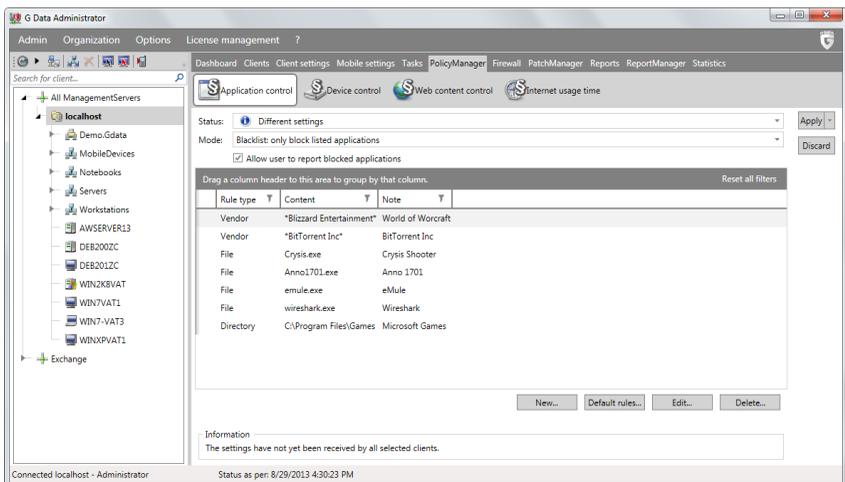
A new rule can be defined using the **New** button. Rules are categorised as one of three types:

- **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 attributes** 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).

4.4.6.2. 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.

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.

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.

4.4.6.3. 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.

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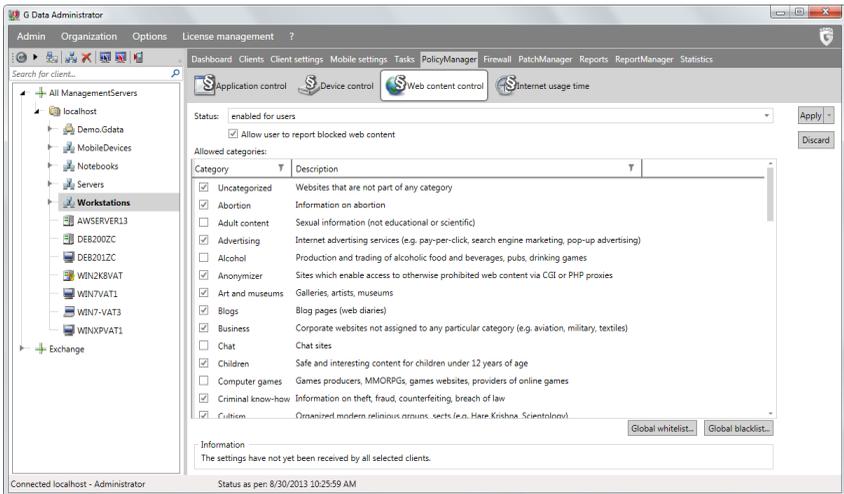
Using the **Global blacklist**, it is possible to ensure that certain websites are blocked company-wide across the entire network, regardless of any settings that have been made under Allowed categories. To do this, simply enter the address which you would like to block under **URLs**, then click on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

4.4.6.4. 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.

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.
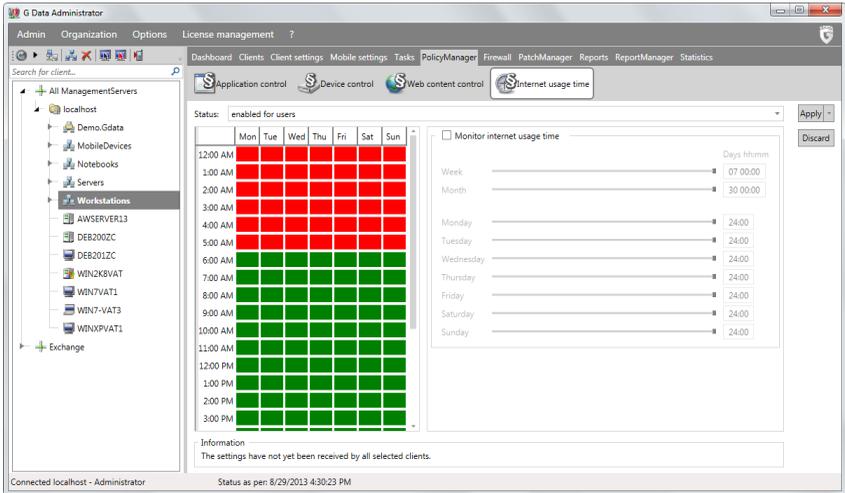
4.4.7. Firewall

The Firewall module is 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.

4.4.7.1. 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 network zones.

Several general firewall settings can be configured:

- **Enable G Data Firewall**: Enable 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.

- **Allow user to 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.

- **Allow user to change the off-site configuration**: Allow users to configure their firewall when they are outside of the network. As soon as the mobile computer reconnects 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.
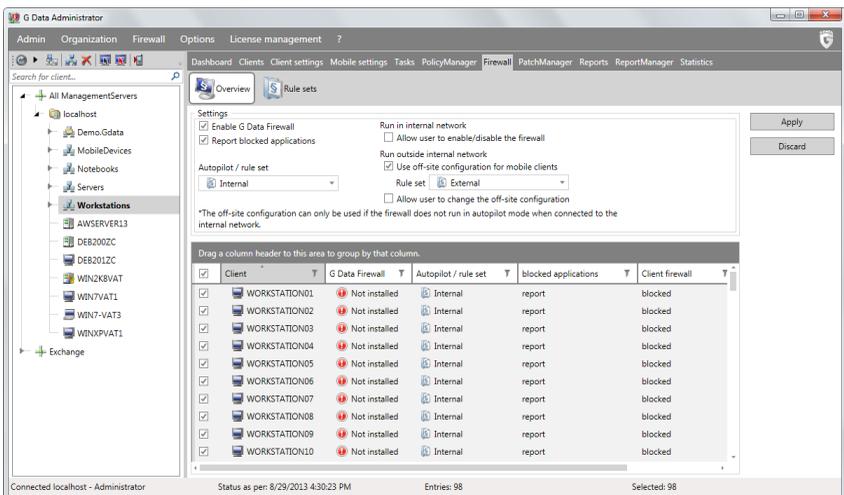
All client computers or clients in a selected group are displayed in the overview. This enables you to see at a glance how the client firewall has been configured and to make changes directly. The list contains the following data:

- **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 mode**: 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 off-site 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**: Initiate a remote installation of G Data Firewall. The system requirements for a remote installation must be met (see G Data Security Client remote installation).
- **Uninstall G Data Firewall**: Uninstall the client's firewall.

4.4.7.2. Rule sets

On the Rule sets panel you can create rule sets for various network zones. Each rule set can contain any number of firewall rules.
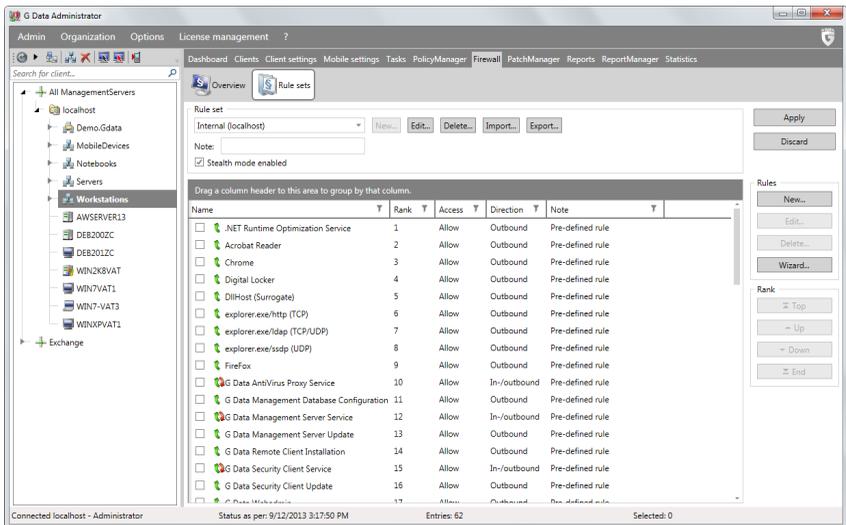
New rule set

Under **Rule set**, click **New** to open the **New rule set** window. Enter a **Name** for the rule set and an optional **Note** or comment. Select **Stealth mode enabled** to block requests to the computer that try to verify a port's accessibility. This makes it difficult for

attackers to obtain system information. After entering this information, the **Rule set for trusted network** window lets you pick one or more default rules to add to the rule set. After confirming the selection with **OK**, the rule set will be shown in the overview. Using the **Edit** button, the rule set's name, note and stealth mode setting can be edited. Click **Delete** to remove the current rule set. Rule sets can be imported and exported as an XML file.
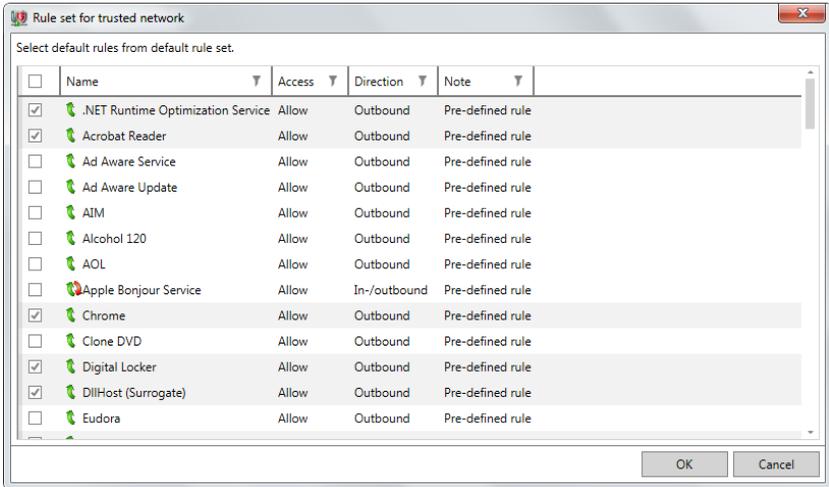

Depending on which rule set you have specified for the relevant network, one rule set (e.g. for untrustworthy networks) may block an application while another (e.g. for trustworthy networks) could grant it full network access. This means you can use a strategic combination of rules to restrict a browser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

New rule/Edit rule

All rules for the current rule set are displayed in the list view. Under **Rules**, use the **New** or **Edit** buttons to add a rule to the current rule set or to edit an existing rule.

- **Name**: For pre-defined and automatically generated rules, this field displays the program name to which the 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.
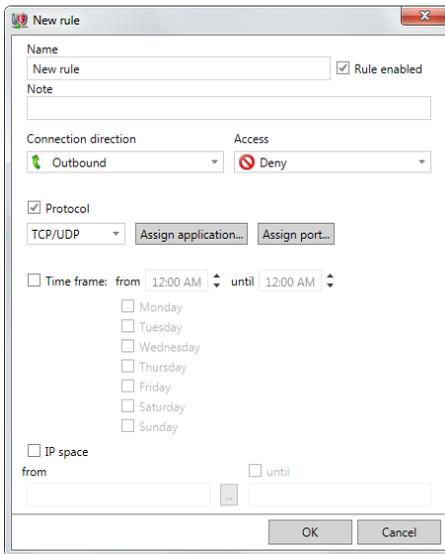
Rule wizard

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.
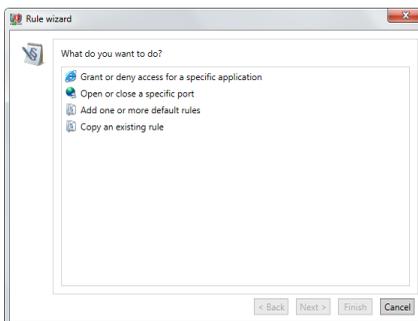
The following actions are available in the Rule wizard:

- **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**

4.4.8. 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.

4.4.8.1. Status overview

The Status 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. By default, it is grouped by Status, Priority, Vendor and Product, to quickly assess whether essential patches have yet been installed or not.

The Status 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 only patches: by default, PatchManager only displays patches and updates. To view other software packages, deselect this option.
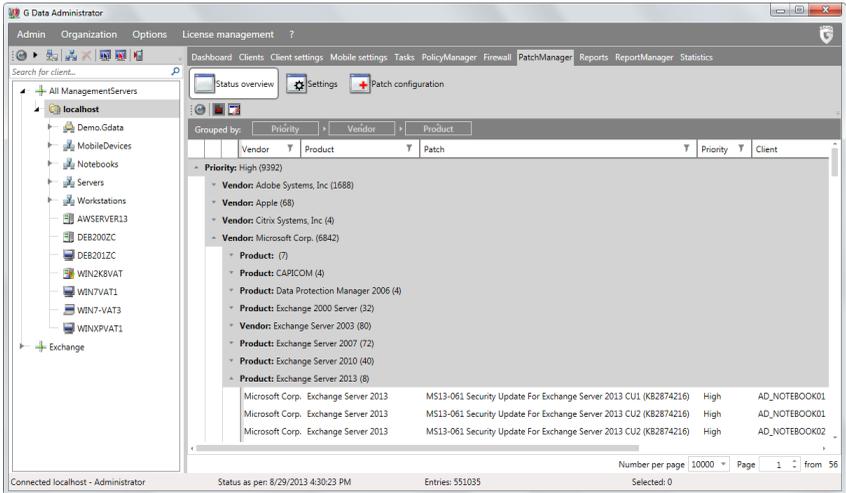
Per patch and client, several types of patching jobs can be planned. Right-click one or multiple patches and click **Check patches for applicability** to run a job that checks if the selected patches apply to the selected clients. The **Software recognition** window pops up and allows you to schedule 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).

4.4.8.2. Settings

The Settings panel controls several options related to patch deployment.

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 **Allow the user to view and request patches**. To allow a client to (temporarily) refuse patch installation, tick **Allow the user to refuse patch installation**. You can select how many refusals are allowed until installation is forced, and how often patch installation should be attempted.
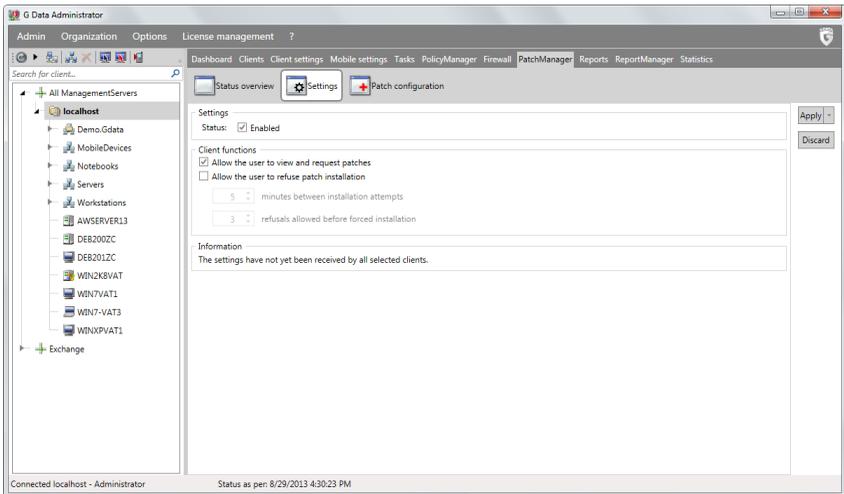
4.4.8.3. Patch configuration

The Patch configuration panel lists all available patches and lets you configure them. By default, patches are grouped by Vendor, Product and Priority, allowing you to quickly find patches by product.

By default, patches are grouped by Vendor, Product and Priority, allowing you to quickly find patches by product. 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 only patches**: 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.
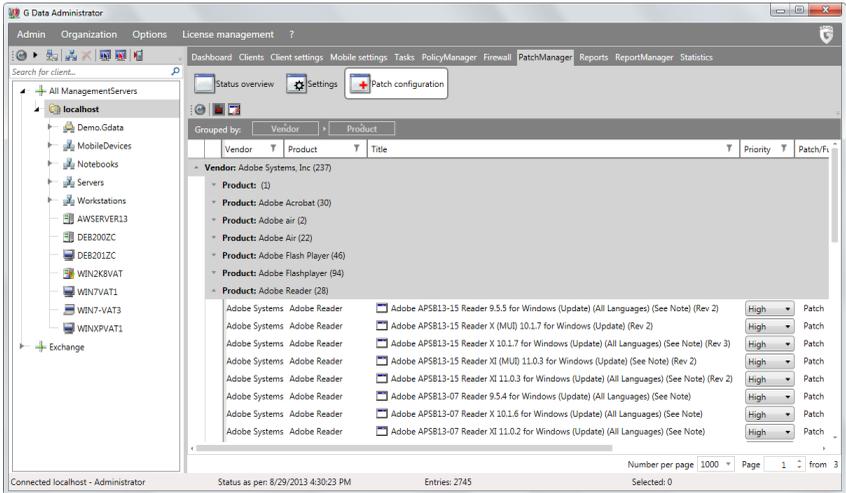
To put one or more patches on the blacklist, right click it and select **Put patches on the blacklist** (this will update their status in the Blacklisted column to *Yes*). To remove a patch from the blacklist, right click it and select **Remove patches from the blacklist**. To view more information and 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**).

4.4.9. 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 report type is displayed in the **Status** column (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 opening the PatchManager module to select the patch and client.
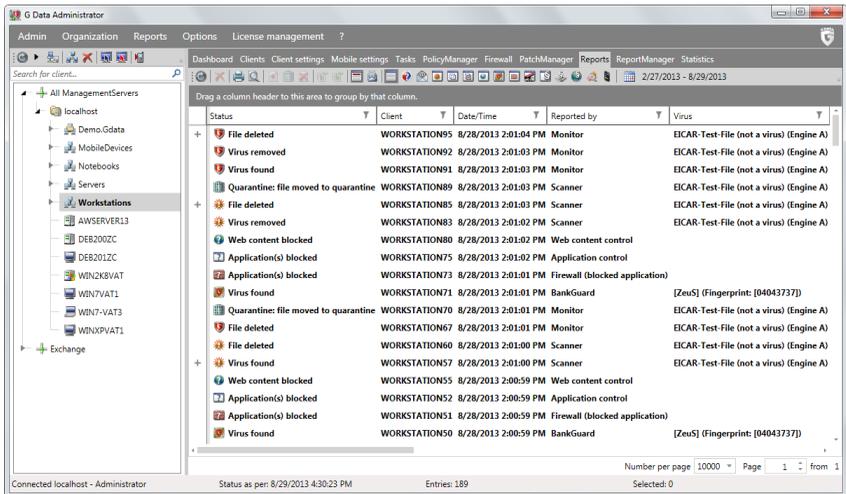
In the menu bar, an additional menu entry is available for the Reports module. For functions that operate with files (delete, move back, etc.), you must select one or more files in the list. You can select the following functions:

- **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 via the Quarantine function. We will, of course, treat the data you have sent us with the utmost confidentiality and discretion.

- **Quarantine: delete file and report**

- **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.

The toolbar of the Reports module offers a wide array of options and filter settings:

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

All reports

Only errors and information

Only email reports

Only reports of non-removed viruses

Only quarantine reports

Only quarantine contents

Only HTTP reports

Only BankGuard reports

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

Only BehaviorBlocker reports

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

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

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

Only Update/Patch Management reports

Only MobileDeviceManagement reports

4.4.10. 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.

Refresh: refresh the list.

Delete: delete the selected report definition(s).

Add new report schedule: define a new report and schedule a reporting job.
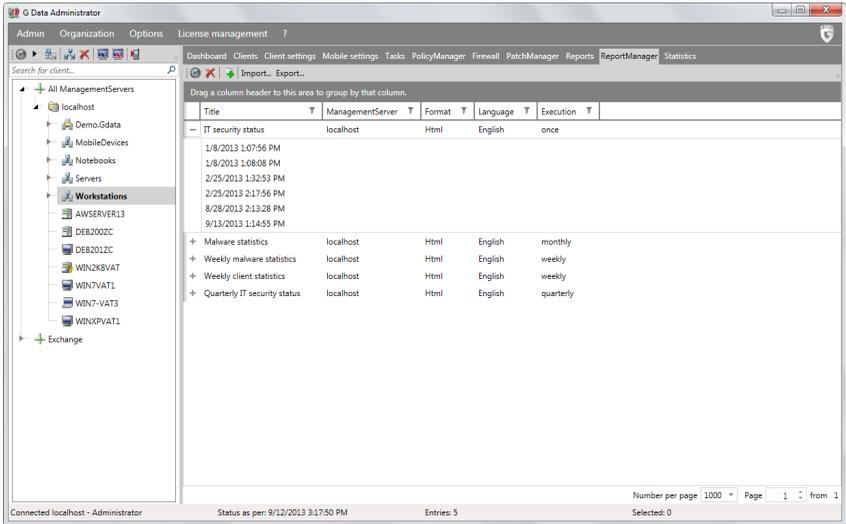
To backup report definitions, click **Export** to save them as a .dbdat file. Click **Import** to restore definitions. Right-click one or more report definitions to **delete** them or click **Execute immediately** to run the reporting job immediately. Click **Properties** to edit a report.

4.4.10.1. 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.

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.
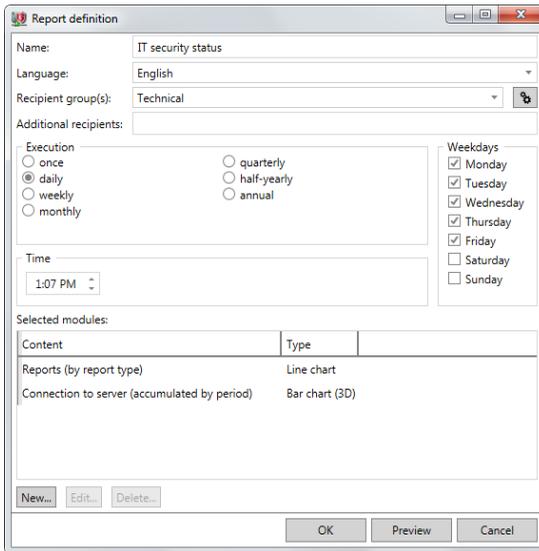
To add a module to the report, click **New** at the bottom of the screen to open the **Module selection** screen. Availability of the modules depends on the product version that you are using. The report modules have been divided into three categories: **Client general**, **client protection** and **PatchManager**. 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.
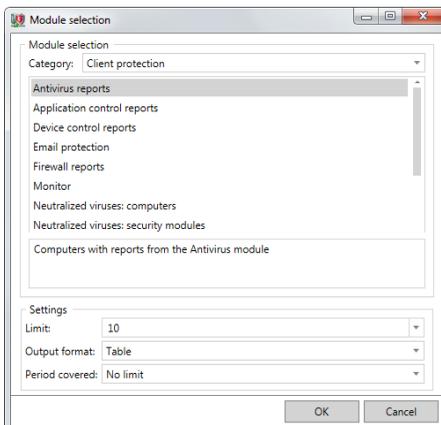
When a reporting job has been run, the resulting report will appear in the ReportManager overview and it will be sent to the defined recipients. Expand the report definition to see the full report history. Double click on an instance to open the associated report.

The Report history and Report preview functions require Internet Explorer 8 or higher to be installed on the machine from which G Data Administrator is run.

4.4.11. 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 neutralized infections**. Select the relevant area in the display to view the data.
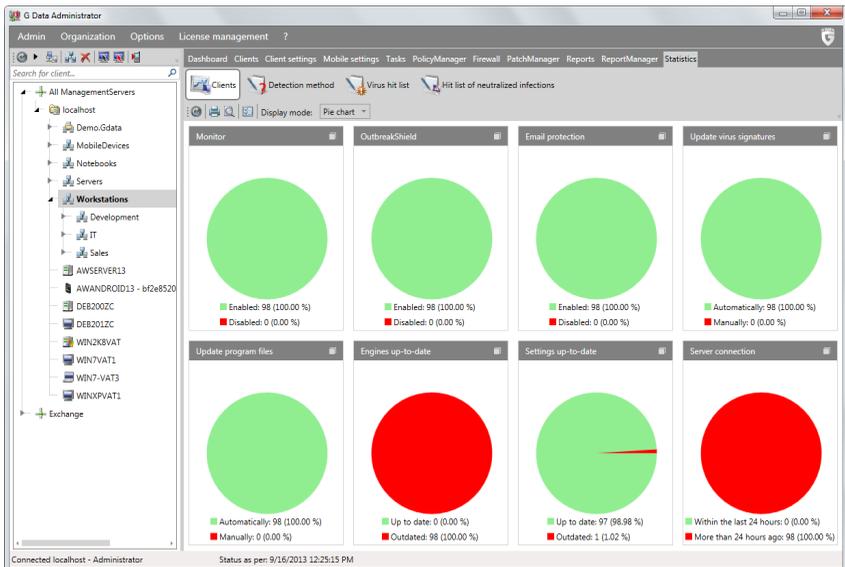
5. G Data WebAdministrator

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.

5.1. 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.

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 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.

5.2. 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.
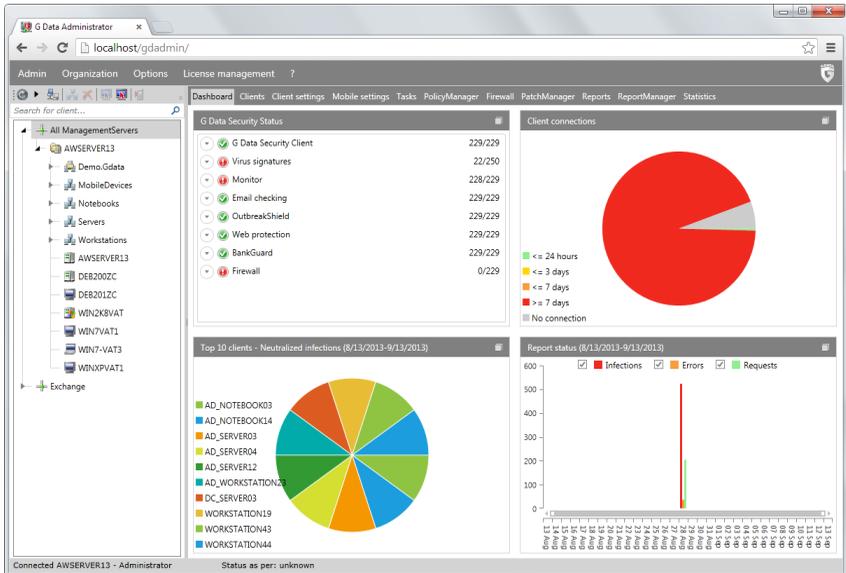
The functionality of WebAdministrator is identical to G Data Administrator. Please refer to the appropriate chapter for an in-depth overview.

6. 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.

6.1. 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/*).

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 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.

6.2. 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.

6.2.1. 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.
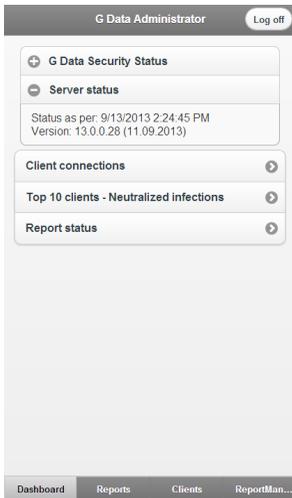
Select **G Data Security Status** to view extensive information about the status of server and clients. MobileAdministrator will show you how many machines have the G Data Security Client installed, as well as information about (outdated) virus signatures and program components such as monitor, email 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**.
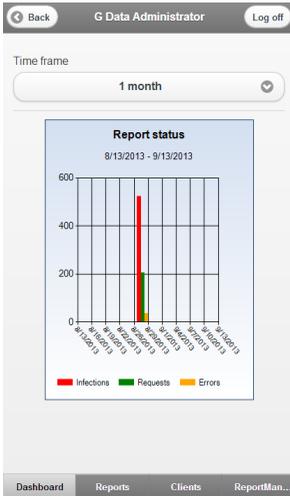
Statistics are available under **Client connections** and **Top 10 clients - Repelled infections**. Tap **Report status** to check on infection, request and error reports.

6.2.2. 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.
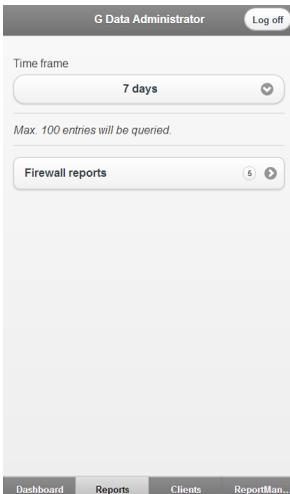
Select the period (**Time frame**) for which you want to view reports (1 day, 7 days or 1 month). MobileAdministrator will return the different categories for which reports are available. Tap a category to view the individual reports available. Reports can be filtered by name. Any report can be opened to check on further details and take action, if necessary.

6.2.3. 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.
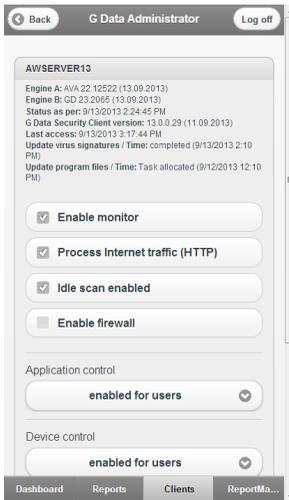
The Clients overview provides a list of all machines that are being managed by G Data ManagementServer. The list can be filtered by name. By selecting an individual machine, you can check several statistics about versions and updates. Additionally, several security settings can be edited. Enable or disable **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.

6.2.4. ReportManager

ReportManager is the mobile version of the **ReportManager** module in G Data Administrator. It allows you to configure, schedule and preview reporting jobs.
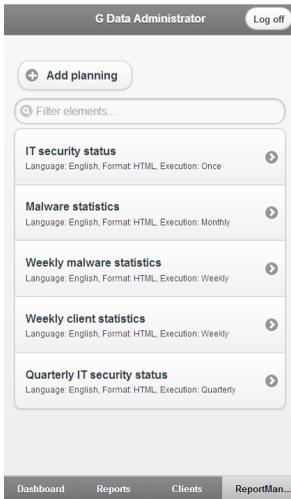
To add a new job, tap **Add planning**. Existing reporting jobs are listed in the main view of ReportManager and can be edited by tapping them. The job view lets you edit all aspects of the job. Enter a **name**, define the **language** and select a **recipient group** or enter additional recipient(s). 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.

7. 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).

7.1. 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 Security Client icon to open a context menu which contains the following options.

7.1.1. 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.
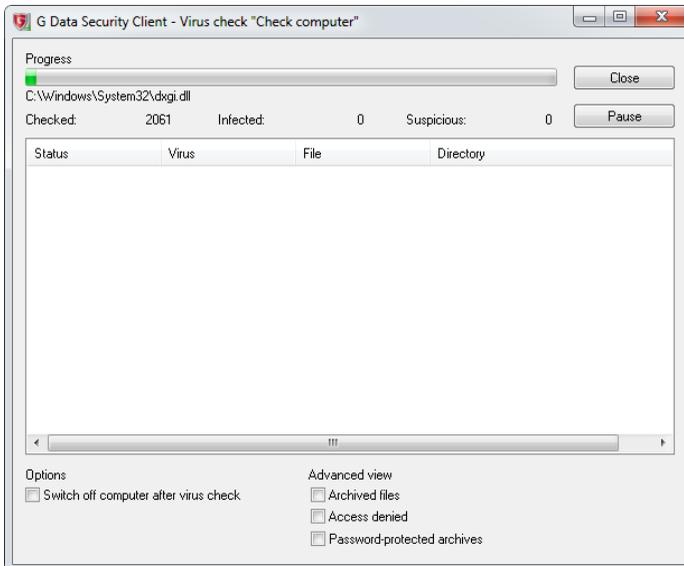
The user can check removable devices, CDs/DVDs, memory, the Autostart area, and individual files or directories. In this way, notebook users who only rarely connect their computers to the company network can prevent a virus attack in a targeted manner. Clients can use the **Options** window to configure 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 **Allow user to 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 **Allow user to 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).

The Virus check system tray menu option can be enabled or disabled in G Data Administrator under **Client settings** > **General** > **Client functions**.

7.1.2. 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). 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.

The Disable monitor system tray menu option can be enabled or disabled in G Data Administrator under **Client settings** > **General** > **Client functions**.
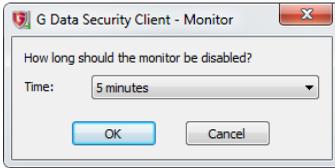
7.1.3. Options

Using the Options window, the user can configure security for the **Monitor**, **Email**, **Virus check** (local), **Web/IM filtering** and **Spam filter** components. 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**.
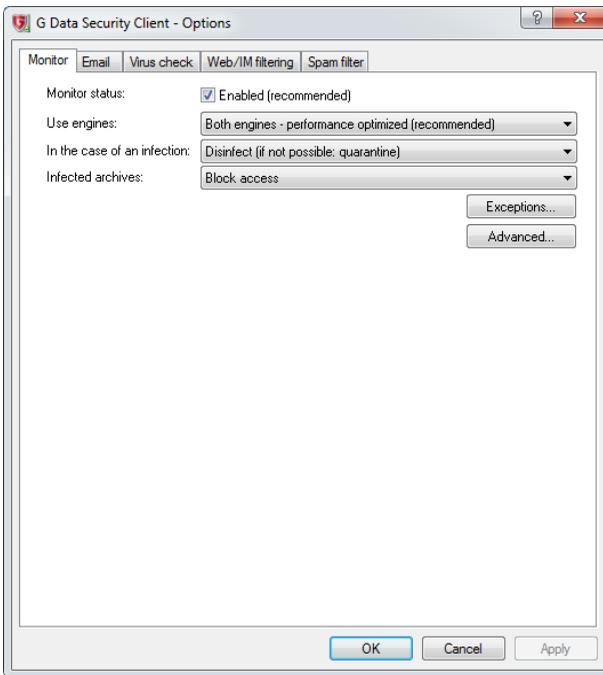
The various tabs of the options menu can be enabled or disabled in G Data Administrator under **Client settings** > **General** > **Client functions**.

7.1.4. 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.

The Quarantine system tray menu option can be enabled or disabled in G Data Administrator under **Client settings** > **General** > **Client functions**.

7.1.5. Updates/Patches

The Updates/Patches window reveals a patch/update overview for the client pc, divided over two tabs.
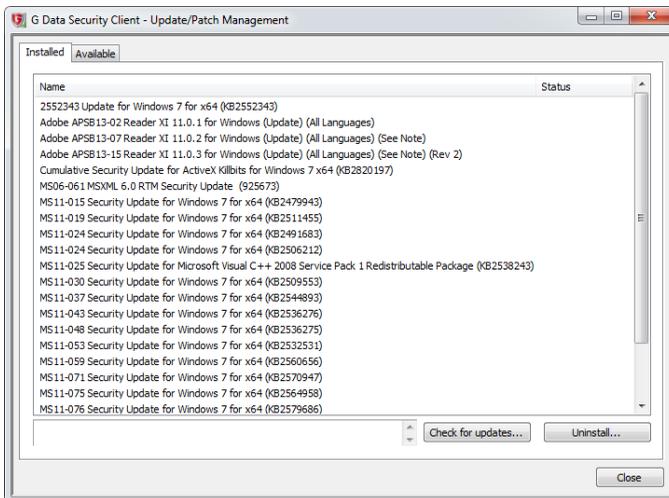
The **Installed** tab shows all patches and updates that have been installed on the system. Double click a patch to view an extended description. If a patch or update seems to be causing problems, users can select it and click **Uninstall** to ask the

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.

The Updates/Patches system tray menu option can be enabled or disabled in G Data Administrator under **PatchManager** > **Settings**.

7.1.6. Internet update

G Data Security Client can be used to carry out virus signature updates from the Internet if no connection to G Data ManagementServer is available. Use the **Settings and scheduling** button to schedule virus updates locally.

The Internet update system tray menu option can be enabled or disabled in G Data Administrator under **Client settings** > **General** > **Client functions**.
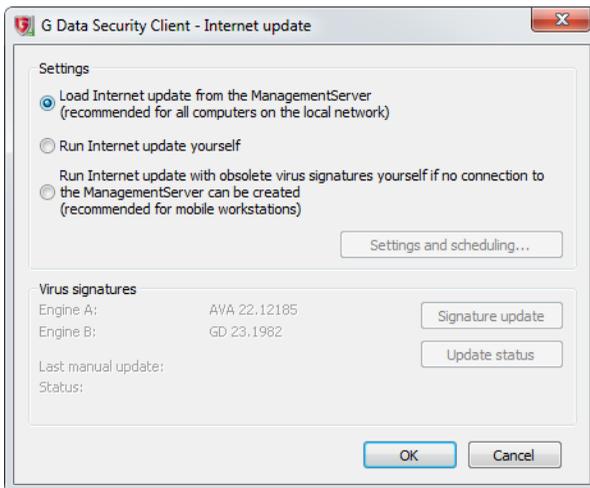
7.1.7. Firewall

The Firewall option loads the firewall's interface. As long as the client is in the G Data ManagementServer network, the firewall will be administered centrally by the server. When the client connects to another network, for example if a laptop is using a private network at home, the firewall interface can be used to configure an off-site configuration. The firewall interface has its own help file, available by pressing F1,

which offers detailed instructions on how to configure it.

The Firewall system tray menu option can be enabled or disabled in G Data Administrator under **Client settings** > **Firewall** > **Overview** by checking **Allow user to change the off-site configuration**.

7.1.8. Disable firewall

Using the option Disable firewall, end users can disable G Data Firewall completely, even if they are connected to the enterprise network. If the firewall has been disabled, it can be re-enabled by clicking the option Enable firewall in the system tray menu.

The Disable firewall system tray menu option can be enabled or disabled in G Data Administrator under **Client settings** > **Firewall** > **Overview** by checking **Allow user to enable/disable the firewall**.

7.1.9. About

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

8. G Data MailSecurity MailGateway

G Data MailSecurity MailGateway provides complete protection of your corporate email communication by scanning all incoming and outgoing e-mail as an independent gateway. MailSecurity MailGateway runs in the background, but 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.

9. 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.
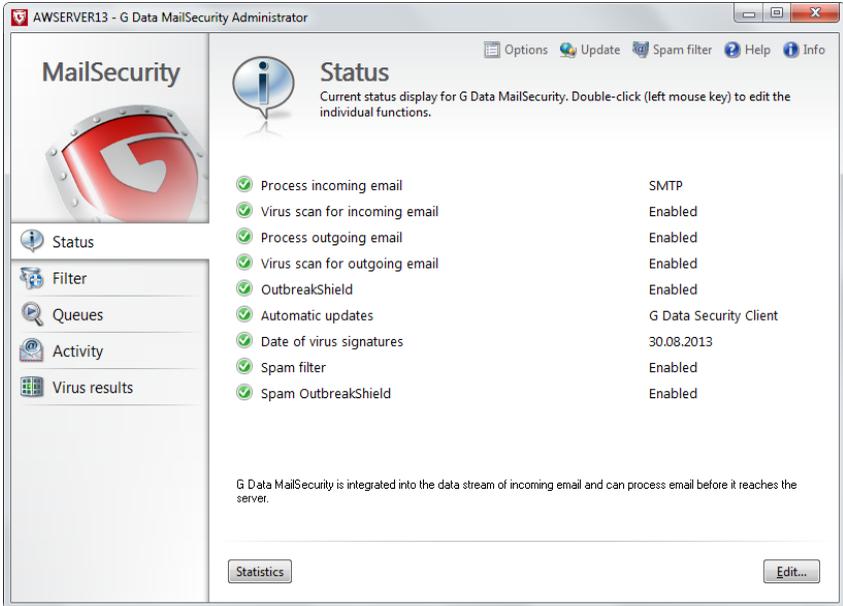
9.1. Starting G Data MailSecurity Administrator

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, 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.

At the first login, 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.

9.2. 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.

9.2.1. 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.

9.2.1.1. Incoming (SMTP)

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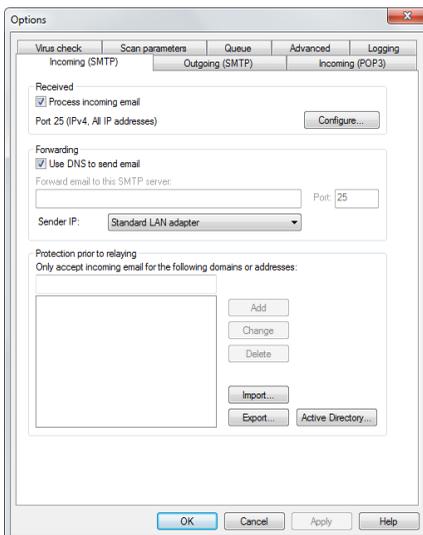
Received

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 for the following domains or adresses**. 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.

9.2.1.2. Outgoing (SMTP)

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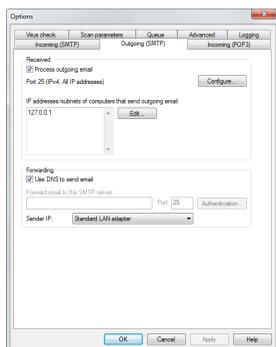
Received

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.

9.2.1.3. Incoming (POP3)

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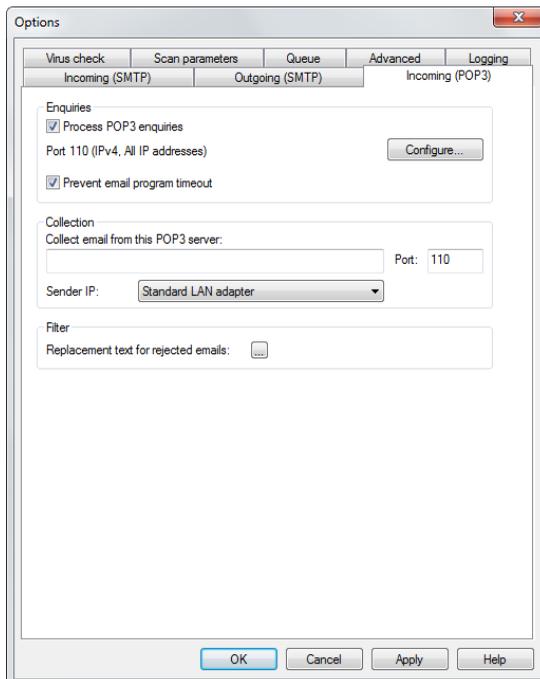
Enquiries

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

9.2.1.4. Virus check

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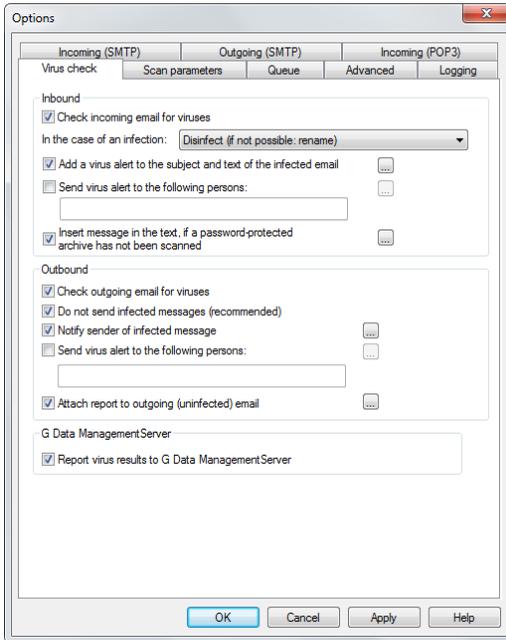
Inbound

In almost all cases, you should enable **Check incoming email for viruses** and also check which option you want to use **in the 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 network 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 **Subject** and **Email text** fields - the same wildcards as the ones that are used in the **Incoming (POP3) Filter** settings.

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 **Subject** and **Email text** fields - the same wildcards as the ones that are used in the **Incoming (POP3) Filter** settings.

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 ManagementServer

If MailGateway is being operated as part of a G Data business solution, you can enable **Report virus results to G Data ManagementServer** to make sure that G Data ManagementServer is informed of MailGateway virus discoveries, so that it can provide you with a comprehensive overview of virus infections in your network.

9.2.1.5. 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.

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 **Login 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.

- **Phishing protection**: Enable Phishing protection to filter out emails that try to obtain passwords, credit card numbers, or other personally identifiable information by posing as an email from a legitimate institution.
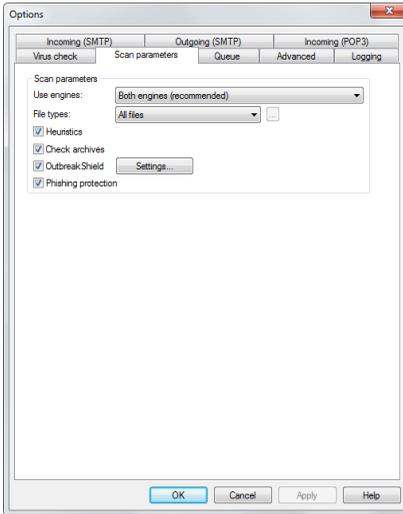
9.2.1.6. Queue

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.
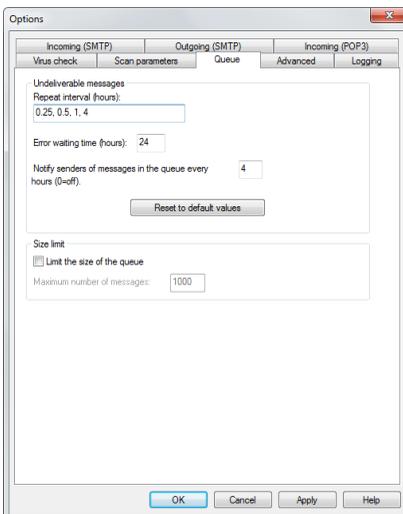
Undeliverable messages

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**, where ... 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.

9.2.1.7. Advanced

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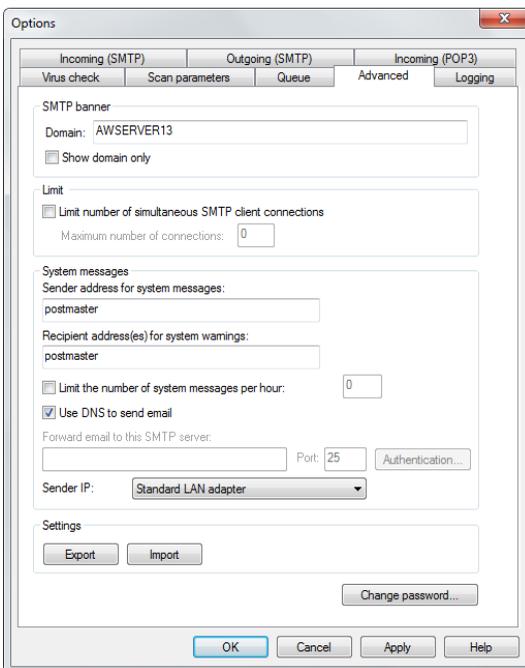
SMTP banner

By default, the server's computer name is entered as **Domain**. When sending outgoing mail using DNS, the fully qualified domain name (FQDN) has to be entered here to enable reverse lookups. Check **Show domain only** to suppress the publication of server version information in communication with other servers.

Limit

To limit the number of SMTP connections that G Data MailSecurity processes simultaneously, please check **Limit number of simultaneous 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.

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.

9.2.1.8. 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.

9.2.2. 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.
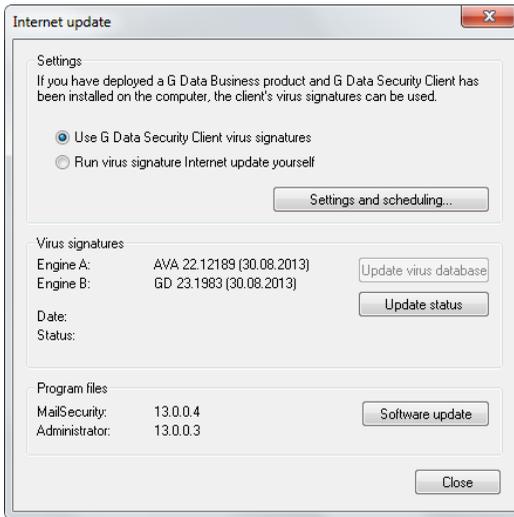
9.2.2.1. Settings

If MailGateway is being operated as part of a G Data Enterprise solution, you can avoid duplicating the downloads by selecting **Use G Data Security 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).
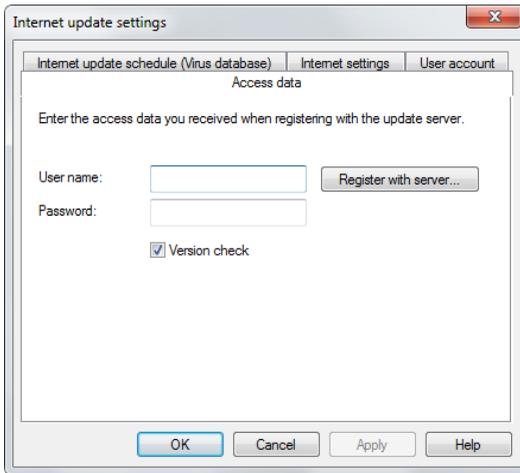
Internet update schedule (Virus database)

The Internet update schedule 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.
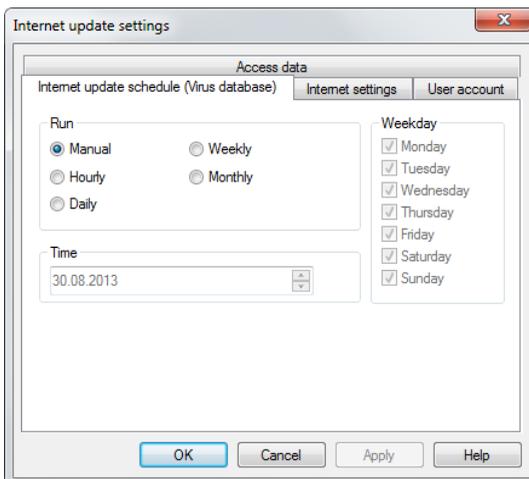
Internet settings

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 optimize connection speed.
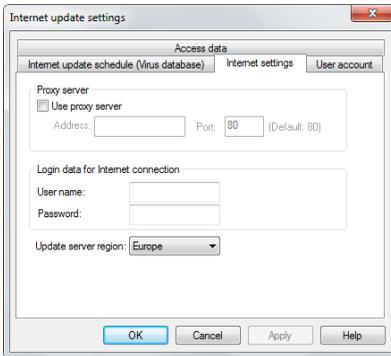
User account

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.
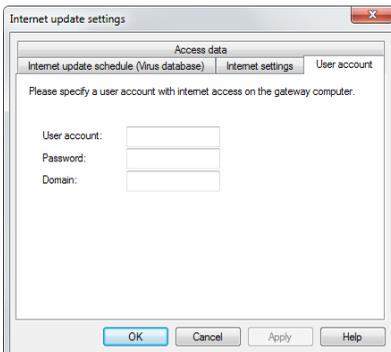
9.2.2.2. Virus signatures

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

9.2.2.3. Program files

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

9.2.3. 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.

9.2.3.1. 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.
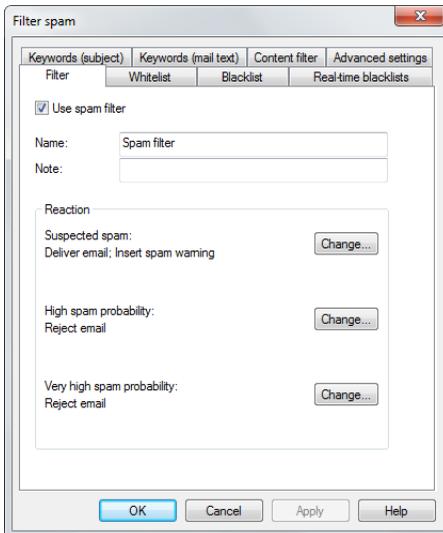
Suspected spam messages, which contain only a few spam characteristics, are not necessarily all spam, but can also be email newsletters or part of a mass emailing that is of interest to the recipient. In such cases, it is recommended that you inform the recipient that the email is suspected spam. **High 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.

9.2.3.2. 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.
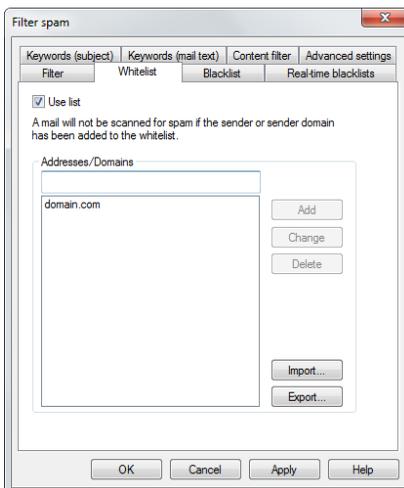
9.2.3.3. Blacklist

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.
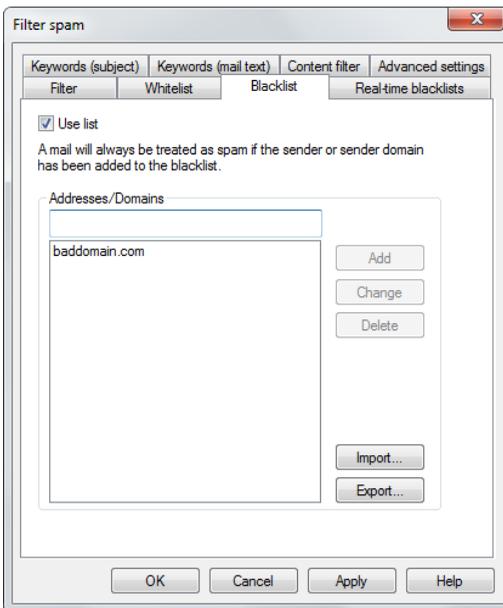
9.2.3.4. Real-time blacklists

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**.
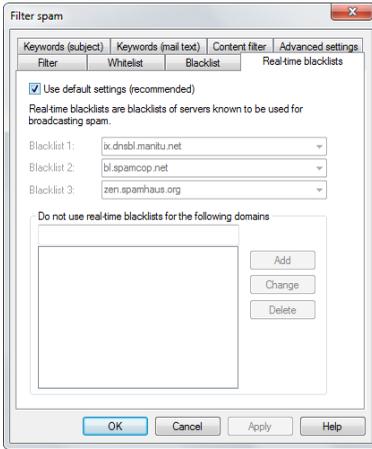
9.2.3.5. Keywords (subject)

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.
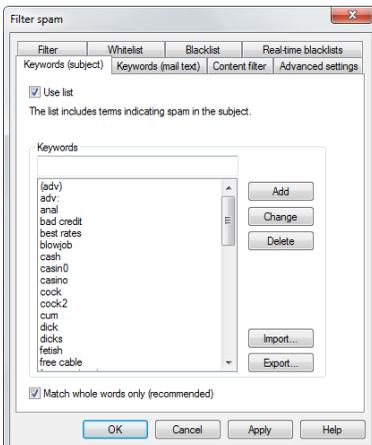
9.2.3.6. Keywords (mail text)

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.
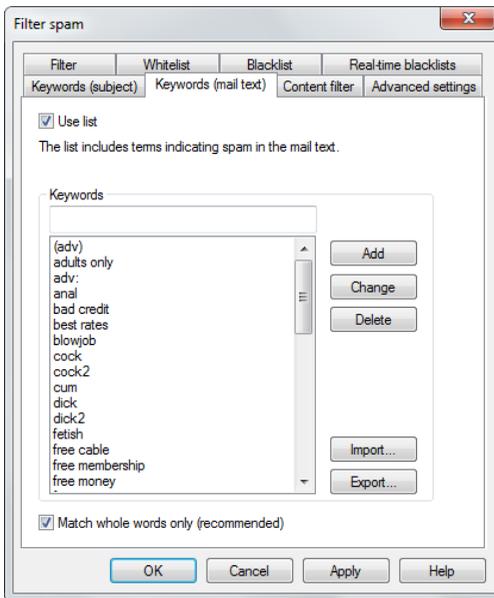
9.2.3.7. Content filter

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.
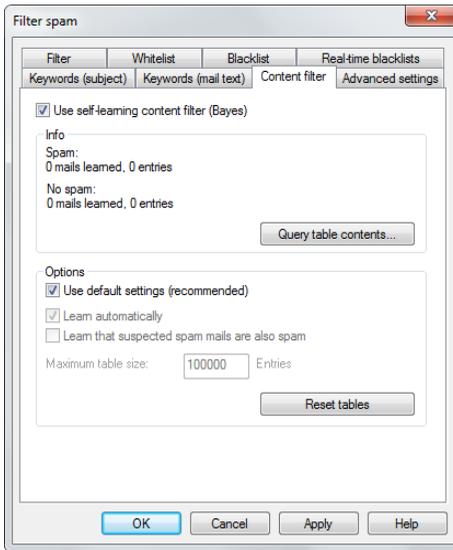
9.2.3.8. Advanced settings

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.
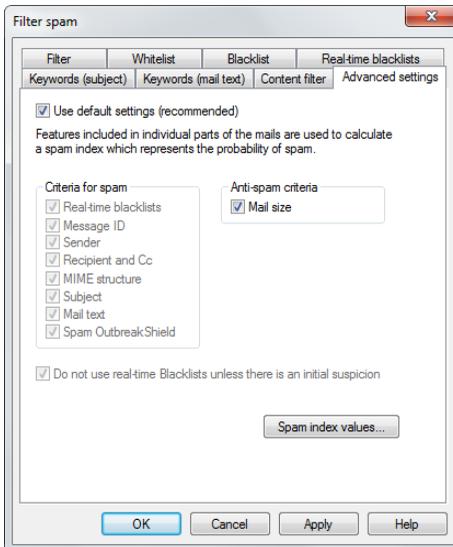
Click **Spam index values** to edit values for the individual attributes that are used to classify emails as Suspected spam, High spam probability or Very high spam probability. It is recommended to leave the option **Use default settings** checked.

9.3. 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.

9.3.1. Status

In the Status module, you will find basic information about the current status of your system and MailGateway.
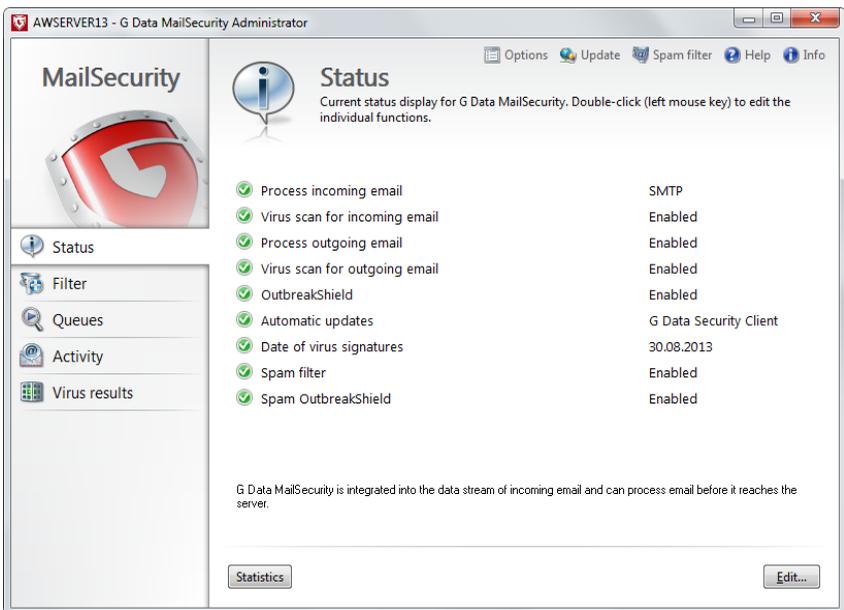
As long as the G Data MailSecurity virus protection is optimally configured, you will see a green icon to the left of the listed entries.

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: **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: **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**.

9.3.2. 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.
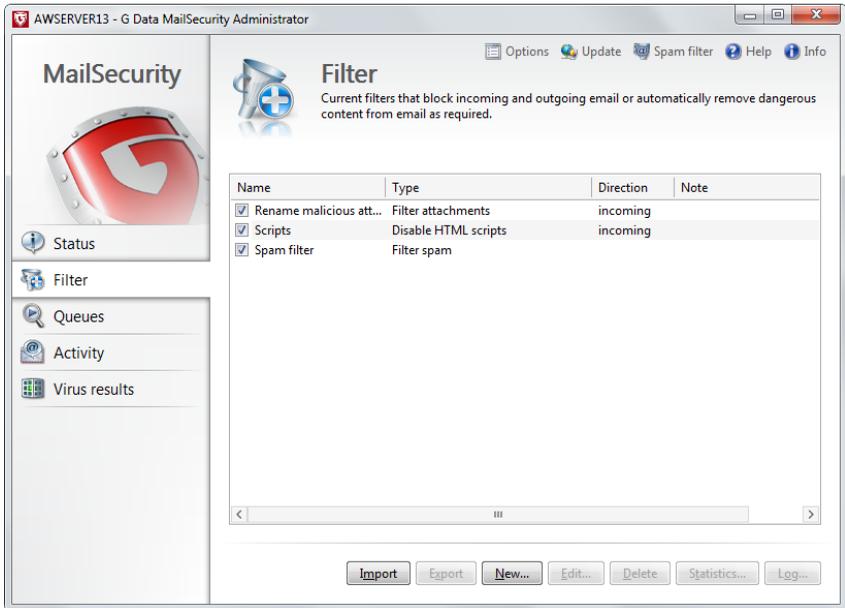
- **Import**: Import filter XML files to restore a backup or reuse filters from other computers.

- **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**: Create new filter rules. 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**: Edit existing filters.

- **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.

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. Wildcards can be used to add information to the **Subject** and **Email text** fields - the same wildcards as the ones that are used in the **Incoming (POP3) Filter** settings.

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

9.3.2.1. Filter read receipt

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

9.3.2.2. 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.

9.3.2.3. 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.

9.3.2.4. 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 a SQL database has been installed on the server.

9.3.2.5. 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.

9.3.2.6. 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).

9.3.2.7. 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.

9.3.2.8. 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).

9.3.2.9. 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.

9.3.2.10. 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 or allow 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 or allowed IP addresses. You can also export the list of IP addresses as a text file or import a text file with IP addresses.

9.3.2.11. 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.

9.3.3. 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.

9.3.4. 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).

9.3.5. 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.

10. G Data Internet Security for Android

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

10.1. Security

The modules listed under Security bundle all preventive measures that Internet Security has to offer. They can be managed centrally through G Data Administrator's **Mobile settings** module, or initiated and configured manually (if allowed by the administrator).

10.1.1. Security center

The Security center of G Data Internet Security for Android offers an overview of all essential security features. Warnings such as virus signature update reminders are listed under the heading **Security center**. Under **Messages**, the app lists recent events, such as scan reports and signature update reports. Select a scan report to view its details. Scan reports can be enabled or disabled in the **Settings** module.
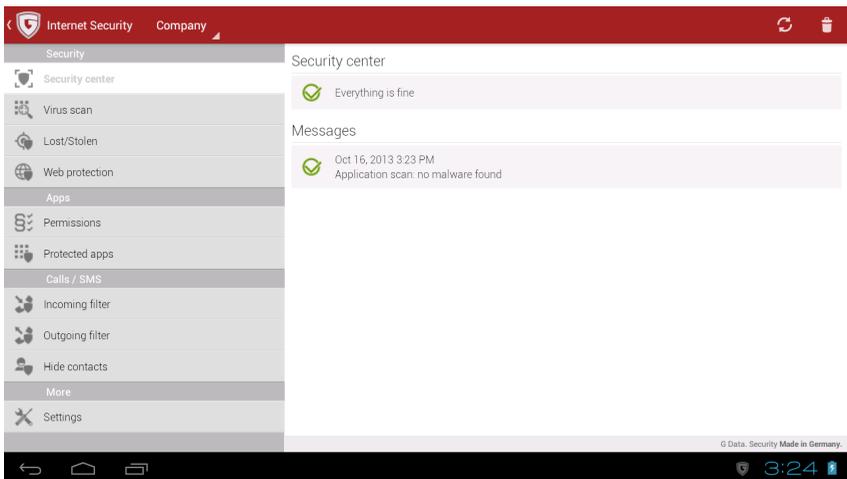

In the top right corner, select the update icon to download the latest virus signatures. The bin icon lets you remove all reports listed under Messages.

10.1.2. 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 analyzes installed applications to identify malware. If any malware is found on your device, Internet Security 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.
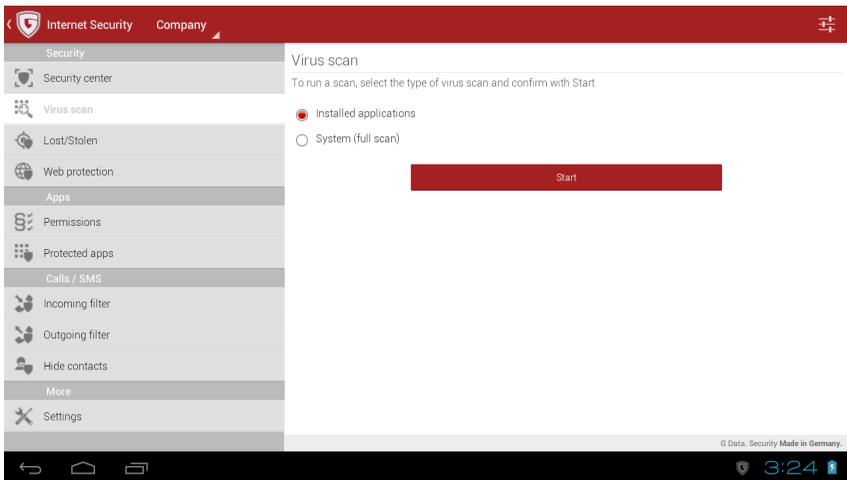
Select the **Settings** icon in the top right corner to open the **Periodic virus scan** settings.

10.1.3. Lost/Stolen

Under Lost/Stolen, two methods of protection lost devices can be configured. The **SMS commands** allow you to configure which commands can be triggered by SMS. **Theft detection** can be used to foil methods commonly used by thieves to evade detection.

The first time you open the Lost/Stolen menu, you will be prompted to enter a **password**, **telephone number** (optional), and **email address** (optional) if they have not already been defined in G Data Administrator under **Mobile settings** > **Anti-theft**. Use the Settings icon in the top right corner if the settings need to be changed afterwards.

10.1.3.1. SMS commands

To protect lost or stolen devices, Internet Security supports various measures that can be remotely activated by SMS.
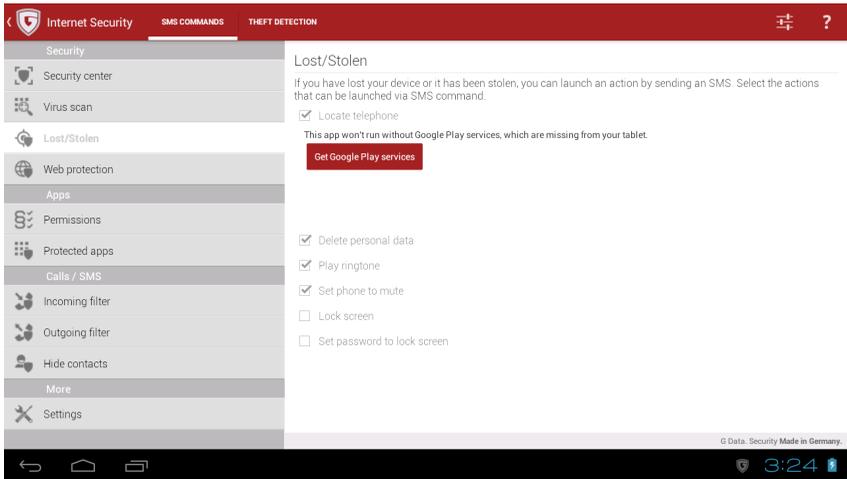
Each security function can be activated by sending a specially crafted SMS message containing the password entered in the **Settings** window. The following options are available:

- **Locate telephone** (also in **Mobile settings** > **Anti-theft**)
- **Delete personal data** (also in **Mobile settings** > **Anti-theft**)
- **Play ringtone** (also in **Mobile settings** > **Anti-theft**)
- **Set phone to mute** (also in **Mobile settings** > **Anti-theft**)
- **Lock screen** (also in **Mobile settings** > **Anti-theft**)
- **Set password to lock screen** (also in **Mobile settings** > **Anti-theft**)

10.1.3.2. Theft detection

Thieves usually change a device's SIM card so that it can no longer be contacted on its original phone number. When this happens, remote commands sent by SMS will no longer work. As a countermeasure, using the Theft detection options, you can specify what should happen to the device if the SIM card is changed:

- **Lock phone on SIM change** (also in **Mobile settings** > **Anti-theft**)
- **Locate phone on SIM change** (also in **Mobile settings** > **Anti-theft**)

If you need to change the SIM card yourself, use the option **Please press here if you are planning to change the SIM card**. It will temporarily disable the SIM change detection until the device is rebooted.
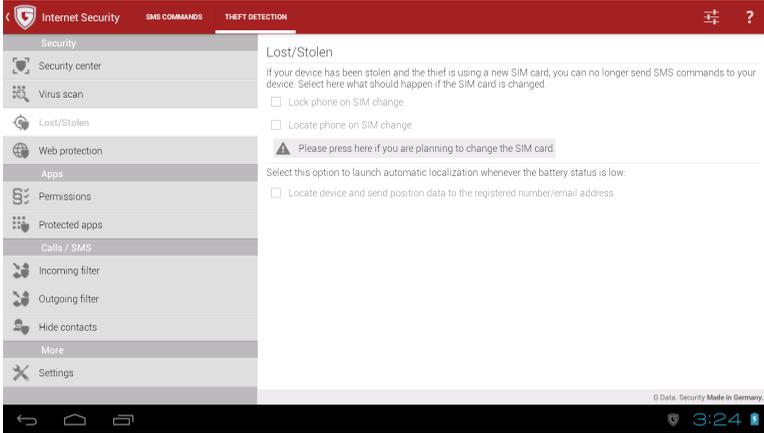
When the battery level is low, the device will no longer automatically detect its location using GPS signals. Select **Locate device and send position data to the registered number/email address** to enable reporting of its last known location whenever the device enters power saving mode.

10.1.4. Web protection

The Web protection module prevents phishing attacks. It blocks phishing websites from being opened in the Android browser and in Chrome. Since some data traffic is required to check the list of phishing websites, the Web protection module can be configured to only look up websites when there is Wi-Fi connectivity (see **Settings** > **Web protection**).
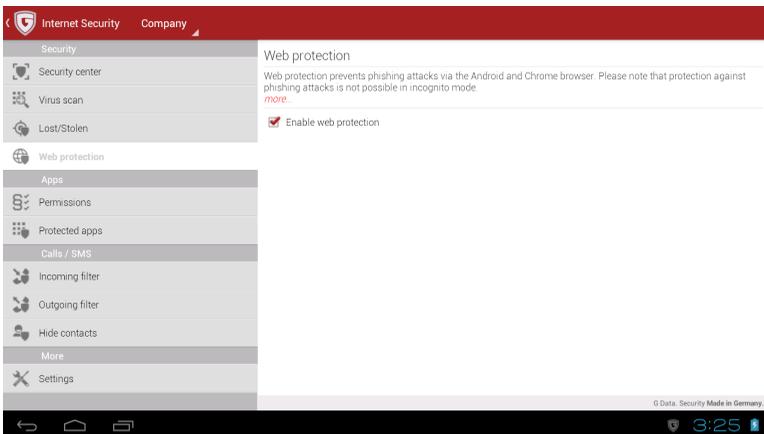
Web protection and its connectivity setting can be managed centrally using G Data Administrator under **Mobile settings** > **General**.

10.2. Apps

The Apps modules let you monitor permissions for installed apps and block apps from being run.

10.2.1. 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 or add them to **Protected apps**.
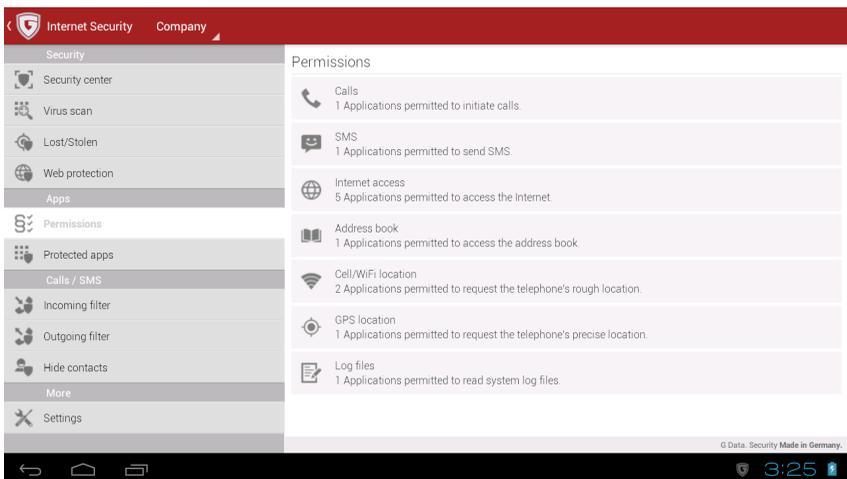
10.2.2. Protected apps

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** and **email address** if they have not already been defined in G Data Administrator under **Mobile settings** > **Apps**, and a **security question**.

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.
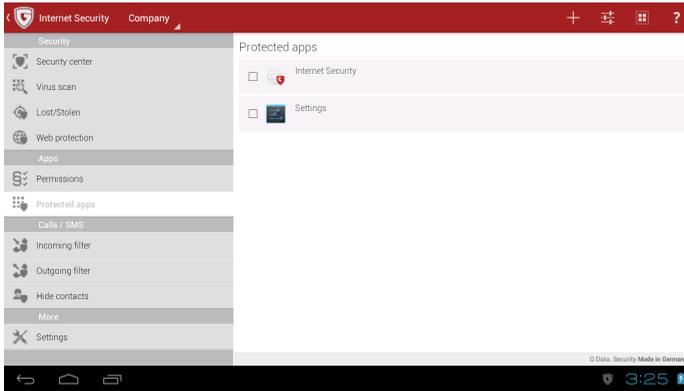
The main panel of Protected apps shows you the list of protected apps. To add an app, tap the **+** button in the top right corner. You can select apps using different views: **Recommended**, **Downloaded**, and **All**. Select an app to add it to the list. It is automatically protected and will ask 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.

10.3. Calls / SMS

The Calls / SMS module combines filtering options with contact management.

10.3.1. Incoming filter

The Incoming filter consists of two separate options. You can choose to enable a **blacklist** or **whitelist** approach to block or allow incoming calls and SMS messages. 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**.
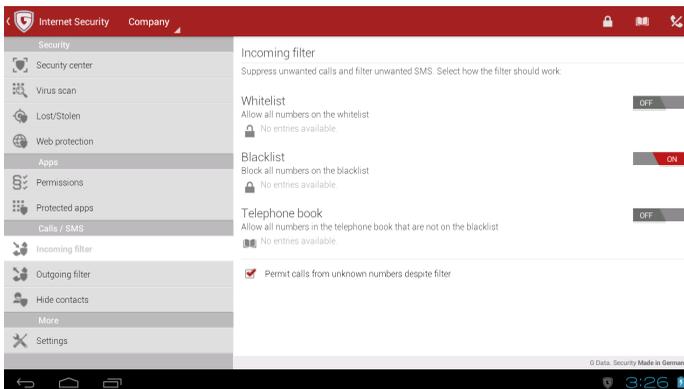
To view the address book, tap the **address book** icon. For a log of suppressed calls and SMS messages, tap the **phone** icon in the top right corner. To view the black- or whitelist, tap the **Lock** icon. To add a number to the list, tap the **+** icon. Phone numbers can be added from the address book or call history. When entering a phone number manually, you can use wild cards to match multiple numbers at once. Asterisks match multiple characters, periods one. For example, entering *0180** will match all phone numbers starting with 0180. Entering *012 345678.* will match phone numbers 012 3456780 through 012 3456789, but not 012 34567800. National and international number formatting are evaluated independently. For example, for an incoming or outgoing call with number 012 3456789, the international format 0049 12 3456789 is evaluated against the wildcard as well. It counts as a match when either or both of the formats match the wildcard.

The Call/SMS filter can be managed centrally in G Data Administrator under **Mobile settings** > **Call filter**.

10.3.2. Outgoing filter

The Outgoing filter lets you define a whitelist and blacklist for outgoing calls. Whitelist and blacklist can be defined using the same options as the **Incoming filter**.
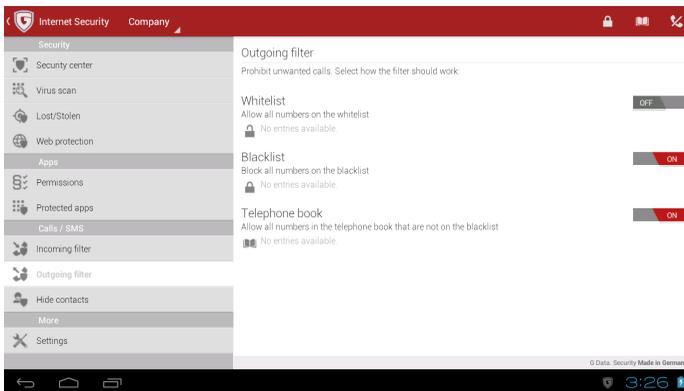
10.3.3. Hide contacts

Contacts and their incoming communication can be hidden. By moving them to a separate G Data phone book, the Hide contacts module effectively blocks access to the contact and all its communication. Advanced contact management can be carried out in G Data Administrator under **Mobile settings** > **Phone book**.
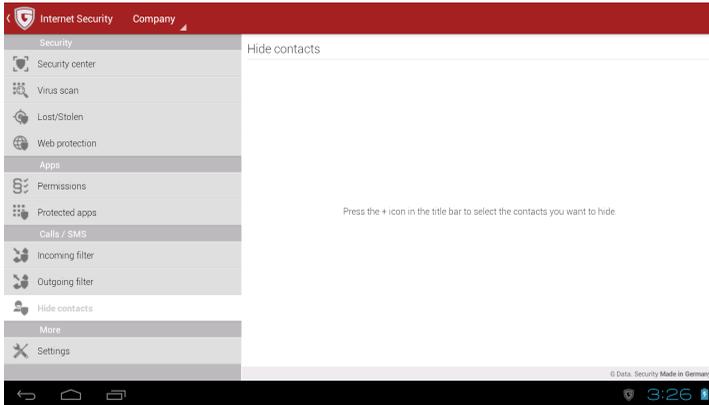
Activate the Hide contacts option to see a list of currently hidden contacts. To add a contact, tap the **+** button. You can select any contact from your address book or call history. After adding a contact, tap its name to edit the protection options. Incoming calls and messages can be intercepted 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, select the contact and choose **Delete entry**.

10.4. Settings

Most of the settings for G Data Internet Security 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.

10.4.1. General

The General section includes tray icon and scan log settings.
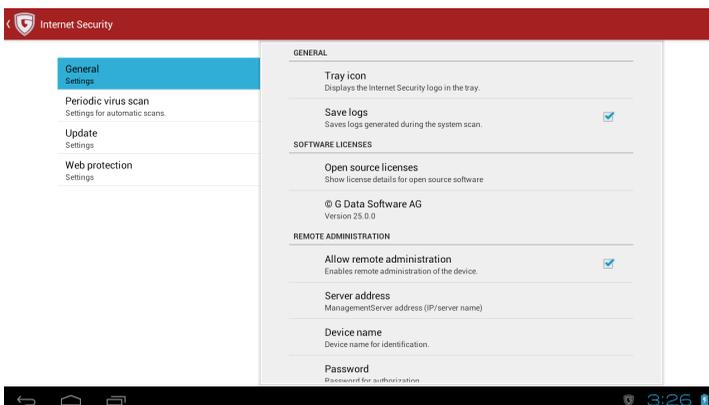
- **Tray icon**: Displays the G Data Internet Security icon in the app tray.
- **Save logs**: Saves scan logs to be viewed in the Logs module.

The Remote administration section can be used to configure server settings to manage the device remotely.

- **Allow remote administration**: Allow Internet Security 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** > **Mobile** window).

10.4.2. Periodic virus scan

The section Periodic virus scan lets you configure settings for virus scans.

- **Automatic scan** (also in **Mobile settings** > **General**)
- **Periodic virus scan** (also in **Mobile settings** > **General**)
- **Battery save mode** (also in **Mobile settings** > **General**)
- **Scan during load process** (also in **Mobile settings** > **General**)
- **Scan frequency** (also in **Mobile settings** > **General**)
- **Type of virus scan** (also in **Mobile settings** > **General**)
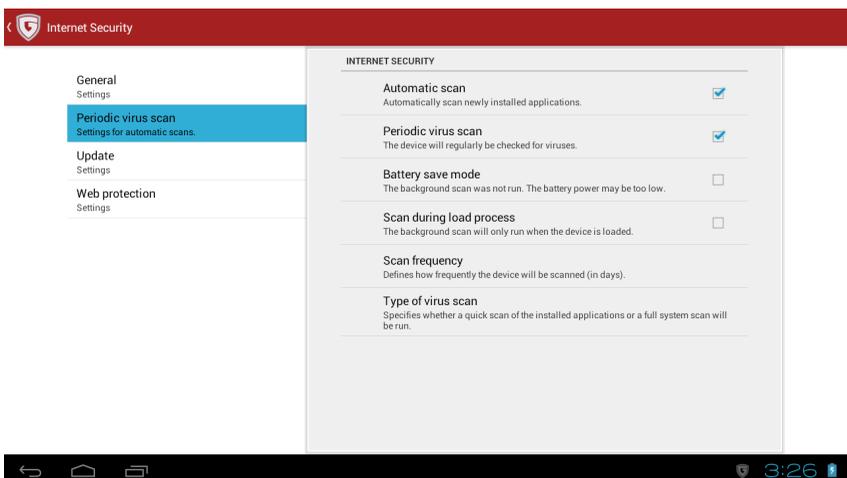
10.4.3. Update

The Update section covers settings related to virus signature updates and the update server region.

- **Automatic update** (also in **Mobile settings** > **General**)
- **Update frequency** (also in **Mobile settings** > **General**)
- **Only via WLAN** (also in **Mobile settings** > **General**)
- **Server region**: Select the update server (not used when Remote Administration is enabled). When Internet Security requests updates for the first time, the nearest update server is automatically selected.
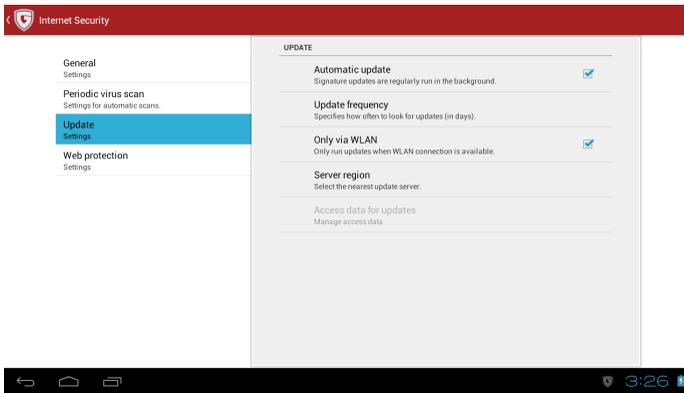
10.4.4. Web protection

The Web protection section includes the possibility to limit web protection to WLAN networks.

- **Only with WLAN** (also in **Mobile settings** > **General**)
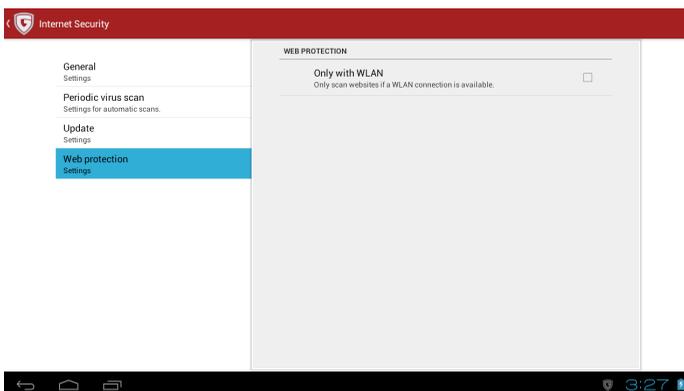
11. Troubleshooting (FAQ)

11.1. Installation

11.1.1. 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 team.

> 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**.

11.1.2. 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.

11.1.3. 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.

11.2. Error messages

11.2.1. 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.

11.2.2. 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.

11.2.3. "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.

11.3. Using Linux

11.3.1. 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.

> **Warning**: 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.

11.4. Other

11.4.1. How can I check whether the clients connect to 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.

11.4.2. 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 team if moving back fails.

11.4.3. Connect to the MMS via its IP address instead of its name

The server name will be requested during the installation, but must be replaced by the IP address if you want to connect to the MMS only via its 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

To make sure 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. 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.

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

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

11.4.5. 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.
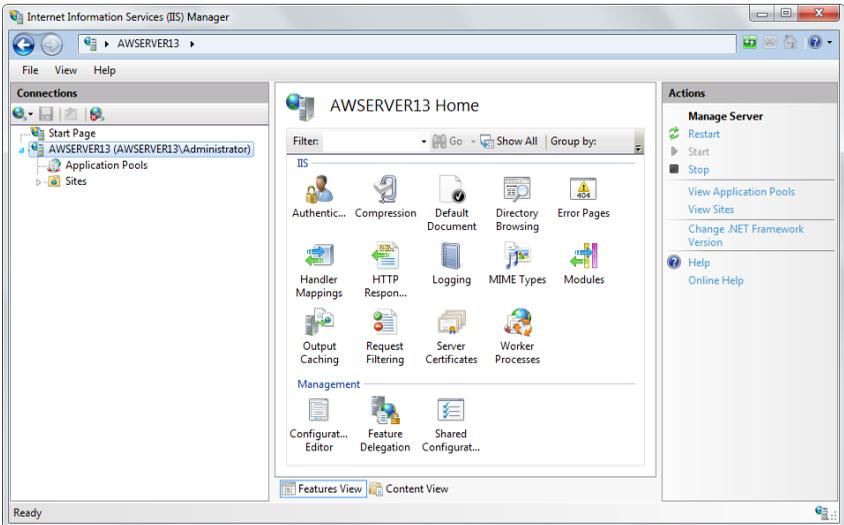
Select your server in the **Connections** panel. In the middle of the screen, navigate to the **IIS** category and double click on **Server Certificates**. On the **Actions** panel, click **Create Self-Signed Certificate**. After entering a friendly name for the certificate, it will be created and listed in the Server Certificates panel. Note that the default expiration date of the certificate is exactly one year ahead of the date of creation.
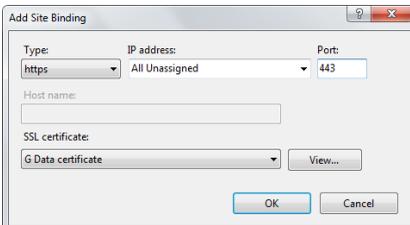
To apply the certificate to site communication, select the appropriate site in the **Connections** panel. On the **Actions** panel at the right, choose **Bindings**. Click **Add** to add a new binding. Select https as **type** and select the certificate you just added in the **SSL certificate** dropdown. 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.

11.4.6. 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).
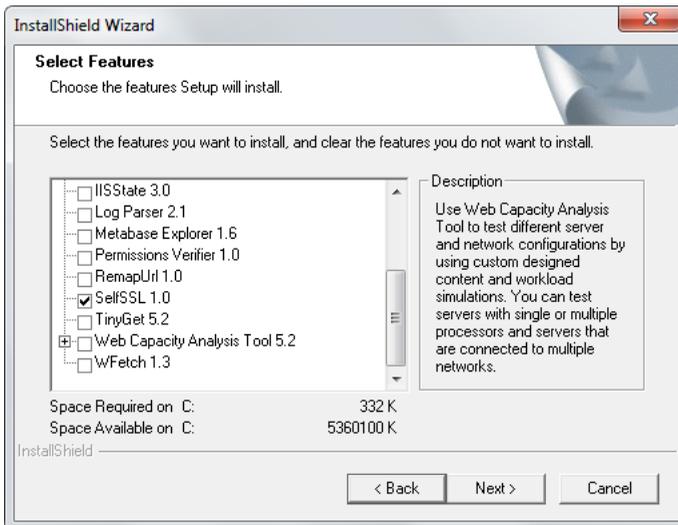
To enable an SSL Server Certificate in IIS 5 (Windows XP) or IIS 6 (Windows Server 2003), you can use the Microsoft tool SelfSSL, which is available in the IIS 6.0 Resource Kit Tools (a free download from the Microsoft website). By performing a **Custom** setup, you can select the tools that you want to install. Select **SelfSSL 1.0**. After installation, open the SelfSSL command prompt through **Start** > **Programs** > **IIS Resources** > **SelfSSL**.

You can assign a self-signed certificate to your website by entering a single command: *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.

12. Legal notices

SharpSerializer

SharpSerializer is distributed under the New BSD License (BSD). Copyright © 2011, Pawel Idzikowski. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

- Neither the name of Polenter - Software Solutions nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Json.NET

Json.NET is distributed under The MIT License (MIT). Copyright © 2007 James Newton-King.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

DotNetZip

DotNetZip is distributed under the Microsoft Public License (Ms-PL).

This license governs use of the accompanying software. If you use the software, you accept this license. If you do not accept the license, do not use the software.

1. Definitions

The terms "reproduce," "reproduction," "derivative works," and "distribution" have the same meaning here as under U.S. copyright law.

A "contribution" is the original software, or any additions or changes to the software.

A "contributor" is any person that distributes its contribution under this license.

"Licensed patents" are a contributor's patent claims that read directly on its contribution.

2. Grant of Rights

(A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create.

(B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free license under its licensed patents to make, have made, use, sell, offer for sale, import, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

3. Conditions and Limitations

(A) No Trademark License- This license does not grant you rights to use any contributors' name, logo, or trademarks.

(B) If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.

(C) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

(D) If you distribute any portion of the software in source code form, you may do so only under this license by including a complete copy of this license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only do so under a license that complies with this license.

(E) The software is licensed "as-is." You bear the risk of using it. The contributors give no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

PhoneNumbers.dll / PushSharp

PhoneNumbers.dll and PushSharp are distributed under the Apache License 2.0 (www.apache.org/licenses).

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works

shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

You must give any other recipients of the Work or Derivative Works a copy of this License; and

You must cause any modified files to carry prominent notices stating that You changed the files; and

You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service

marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

Index

Notes