G DATA
SECURITY SOFTWARE

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 solutions' 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

1.1. Documentation

G DATA business software documentation is available as a 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.

1.2. Support

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

- USA: www.gdata-software.com
- United Kingdom: www.gdatasoftware.co.uk
- International: www.gdatasoftware.com

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

- The version number of G DATA Administrator, which can be found in the help menu.
- The serial number or the Internet Update user name. The serial number can be found in the order confirmation. When in doubt, contact your reseller or distributor.
- The exact version number of the operating system (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.

1.3. G DATA Security Labs

If you discover a new virus or an unknown phenomenon, always send us the file via the Quarantine function, which can be found in G DATA Administrator under **Security events**. Right click on any reported file and choose **Quarantine: Send to G DATA Security Labs**. We will, of course, treat the data you have sent us with the utmost confidentiality and discretion.

1.4. G DATA business solutions

This manual 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 solution, visit our **website** to obtain information about software upgrades.

2. Installation

Start Windows and insert the G DATA installation medium. An installation window will open automatically, which allows you to select which of the G DATA software components you want to install. If you obtained a download version of the software, extract all files and launch Setup.exe. To help install the software on other machines, the extracted files can be burned to a DVD or copied to a USB stick. 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. The following components can be installed:
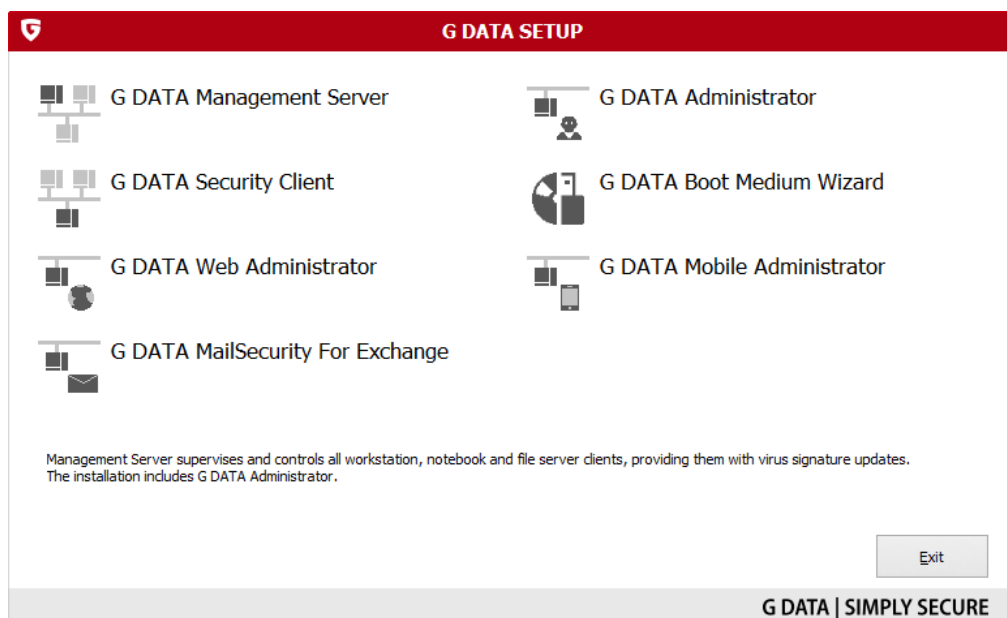
- **G DATA ManagementServer**: Install this component first. G DATA ManagementServer will be used to manage all G DATA-related settings and updates. G DATA ManagementServer lies at the core of the G DATA architecture: it administers the clients, automatically requests the latest software and virus signature updates from the G DATA update servers 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. Installing the client software is generally carried out through G DATA Administrator for all clients.

- **G DATA Boot Medium Wizard**: You can use G DATA Boot Medium Wizard to create a bootable CD, DVD or USB stick for basic scanning of your computer. This scan takes place before the operating system is launched and uses up-to-date virus signatures.

- **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 MailSecurity for Exchange**: G DATA MailSecurity for Exchange centrally secures all Exchange-based email traffic. It is available as an **optional module**.
- **G DATA MailSecurity MailGateway**: G DATA MailSecurity MailGateway centrally secures all SMTP- and POP3-based email traffic. It is available as an **optional module** and can be installed from its own installation medium.

2.1. Getting started

In the event of an acute virus threat, first run a **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 its administration component **G DATA Administrator**.

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

3. When G DATA Administrator is first started on the server, the **Server Setup Wizard** is run. It can be used to install **G DATA Security Client** 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 installation medium** or a **client install package**. 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 G DATA client and server updates can be centrally managed. 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 minimum system requirements apply to the G DATA range of solutions:

G DATA ManagementServer

- Operating system: Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Vista, Windows Server 2016, Windows Server 2012 R2, 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 10, Windows 8.1, Windows 8, Windows 7, Windows Vista, Windows XP SP3 (32-bits), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, or Windows Server 2003

G DATA MobileAdministrator

- Operating system: Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, or Windows Server 2008 R2

G DATA Security Client

- Operating system: Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Vista SP1, Windows XP SP3 (32-bits), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, or Windows Server 2003
- RAM: 1 GB

G DATA Security Client for Linux

- Operating system: 32- and 64-bits editions of Debian 7, 8 and 9, OpenSUSE Leap 42.1 (64-bits) and Leap 42.2 (64-bits), Suse Linux Enterprise Server 11 SP4 and 12 (64-bits), Red Hat Enterprise Linux 5.11, 6.6 and 7.0 (64-bits), Ubuntu 14.04.1 LTS and 16.04, CentOS 5.11, 6.6 and 7.0 (64-bits), Fedora 24 and 25

G DATA Security Client for Mac

- Operating system: Mac OS X 10.7 or higher

G DATA Mobile Device Management for Android

- Operating system: Android 4.0 or higher

G DATA Mobile Device Management for iOS

- Operating system: iOS 7.0 or higher

G DATA MailSecurity MailGateway

- Operating system: Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Vista, Windows XP SP3 (32-bits), Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, or Windows Server 2003
- RAM: 1 GB

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

- Mail server: Microsoft Exchange Server 2016, Microsoft Exchange Server 2013, Microsoft Exchange Server 2010, or Microsoft Exchange Server 2007 SP1

G DATA solutions use the TCP/IP protocol for communication between clients and servers.

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. Firewall configuration

If you are using a network-level or software firewall, you may need to make changes to its configuration. Configure your firewall directly after installing G DATA software to make sure that all functions are available.

2.1.2.1. Ports

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

Main/secondary ManagementServer

- Port 80 (TCP)
- Port 443 (TCP)
- Port 7161 (TCP)
- Port 7182 (TCP)
- Port 7183 (TCP)

Subnet servers

- Port 80 (TCP)
- Port 443 (TCP)
- Port 7161 (TCP)

Clients

- Port 7169 (TCP)

MailSecurity MailGateway server

- Port 7182 (TCP)

MailSecurity Exchange plugin

- Port 7171 (TCP)
- Port 7185...7195 (TCP)

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 G DATA ManagementServer (typically C:\Program Files\G Data\G DATA AntiVirus ManagementServer) and open the file Config.xml in a text editor like Notepad. Look for the following settings and change the port 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 443). The ClientHttpsPort value should not be altered, as Android 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 80).

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*.

2.1.2.2. URLs

When using the **PatchManager** module, G DATA ManagementServer needs to be able to download configuration files and patches. If you are using a firewall, traffic between G DATA ManagementServer and the following URLs always needs to be allowed:

- *gdata.cdn.heatsoftware.com*

Depending on the software for which patches will be deployed, traffic between G DATA ManagementServer and the following URLs also needs to be allowed:

- 7-Zip: *http://downloads.sourceforge.net*
- Adobe: *ardownload.adobe.com*, *armdl.adobe.com*, *download.adobe.com*, *swupdl.adobe.com*, *www.adobe.com*
- Microsoft: *go.microsoft.com*, *download.windowsupdate.com*, *www.download.windowsupdate.com*, *download.skype.com*, *download.microsoft.com*
- Mozilla: *http://ftp.mozilla.org*
- UltraVNC: *http://support1.uvnc.com*
- VideoLAN: *http://download.videolan.org*

2.1.3. G DATA boot medium

Viruses that have embedded themselves on a computer may prevent G DATA software from being installed. The G DATA boot medium will help you fight these threats by scanning your computer before the operating system is loaded.

1. **Using the installation medium**: Insert the G DATA installation medium. In the start window that opens, click **Exit** and turn off the computer.
   Using a G DATA boot medium you have created yourself: To create your own G DATA boot CD, DVD or USB stick, you must first install **G DATA Boot Medium Wizard**. The wizard must be run on a system on which G DATA Security Client with up-to-date signatures has been installed. After installing G DATA Boot Medium Wizard, follow its on-screen instructions to create a G DATA boot medium.

2. Restart the computer. The G DATA boot medium's 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 and the G DATA AntiVirus boot medium 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 medium yourself, the virus signatures are the latest ones that the G DATA Security Client had available at the time the boot medium 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 your

G DATA solution, 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.
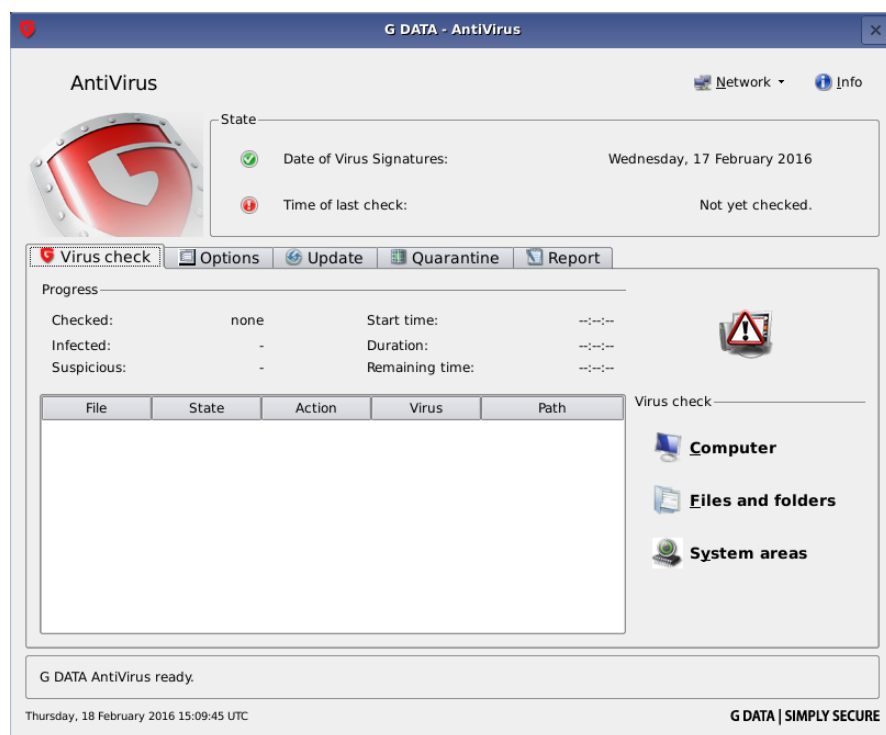
6. If the G DATA software finds any viruses, use the option provided in the program to remove them. Once the virus has been removed successfully, the original file will be restored.

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 medium from the drive or USB port.

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. G DATA Boot Medium Wizard

To create your own G DATA boot medium, you first have to install G DATA Boot Medium 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 installation medium and select **G DATA Boot Medium Wizard**.

Boot Medium Wizard
Welcome!

Boot Medium Wizard helps you create a bootable CD or DVD. Bootable USB sticks can also be created.

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

You can find details on using the boot medium in the instructions.

< Back | Next > | Cancel
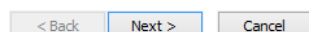
After finishing the installation, navigate to **Start** > **(All) Programs** > **G DATA** > **G DATA BOOT MEDIUM** and click **G Data BootMediumWizard**. The wizard will lead you through the process of creating the G DATA boot medium. It will offer to burn the boot medium directly to the selected CD or DVD burner, to save it to a USB stick or to save it as an ISO image. The ISO file can then be burned using external software, or distributed to network machines digitally.

2.1.3.2. Configure BIOS boot options

If your system will not boot from CD/DVD or USB stick, 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 **USB**, **CD/DVD-ROM, C:**, meaning that the USB port becomes the first boot device, the CD/DVD-ROM drive becomes the second and the hard disk partition with your Windows operating system on it becomes the third.
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 installation medium and select **G DATA ManagementServer**. Ensure that you have closed all open applications, as they may cause conflicts during installation. Select your language and click **Installation** to start the installation wizard. Read the license agreement for the use of this software. Select **I accept the terms in the license agreement** and then click **Next** if you accept the agreement in this form.

The server type selection lets you choose between the following server types:

- **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 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.

- **Secondary server**: When using a standalone SQL database instance, 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.

- **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 server is inaccessible. However, they do not load any virus signature updates autonomously. Enter the server name of the main server under **Main server name**.

   An alternative to installing a subnet server 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 for using a subnet server.

After selecting the server type, decide which database server G DATA ManagementServer should use:

- **Install Microsoft SQL Server 2014 Express**: Choose the SQL Server Express installation if you are newly installing G DATA ManagementServer for a network with less than 1000 clients. Microsoft SQL Server 2014 Express does not support Windows Vista and Windows Server 2008/2003. On those systems, manually install Microsoft SQL Server 2008 R2 Express before installing ManagementServer or use a database instance on another machine and then select the option **Use existing database instance**. More information can be found in the Reference Guide.

- **Use existing database instance**: For larger networks, it is recommended to use an existing Microsoft SQL Server instance. If you are reinstalling G DATA ManagementServer on a server that already has a SQL Server Express installation and a G DATA ManagementServer database, choose the option to use an existing instance. After the installation, you will be able to configure the connection to SQL Server (Express).

The installation is automatically started after confirming the eventual installation of Microsoft SQL Server 2014 Express and/or other prerequisites. After the installation is finished, the G DATA solution should be activated. This enables immediate update downloads upon finishing the installation:

- **Enter a new registration number**: If you are installing G DATA software for the first time, select this option and enter the solution's registration number. You can find the registration number on the order confirmation. In case of doubt contact your G DATA reseller or distributor. Upon entering the registration number, your solution 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 and 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 Business components are available, even if you have purchased G DATA Client Security Business, G DATA Endpoint Protection Business, or any additional modules. The additional components are activated and available as soon as you register the software.

If you chose to use an existing database instance, you can perform the database configuration after the installation has finished. More information about database configuration can be found in the Reference Guide.

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, insert the G DATA installation medium and select **G DATA Administrator**.

Ensure that you have closed all open applications, as they may cause conflicts during the installation. 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, insert the G DATA installation medium and select **G DATA WebAdministrator**.

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 WebAdministrator. 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 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, insert the G DATA installation medium and select **G DATA MobileAdministrator**.

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

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

- **Microsoft Internet Information Services (IIS)**: As MobileAdministrator is a web-based product, the server on which it will be installed should also be running a web server. MobileAdministrator supports Microsoft Internet Information Services (IIS). Ensure you are running IIS before attempting to install MobileAdministrator. 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 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

G DATA Security Client protects and manages Windows network clients and should be installed on each Windows machine. Depending on the deployment scenario, you can choose a **remote installation** (via G DATA Administrator) or a **local installation** (using the G DATA installation medium 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**, remote installations have the following prerequisites:

- A user account with administrative permissions on the client must be entered. The account does not necessarily need to have a password. In that case, however, the target machine must be explicitly configured to allow network logons for accounts without a password. More information can be found in the Reference Guide. To remotely install a subnet server, an account password must be set: an empty password field is not permitted.

- Service Control Manager on the client must be remotely accessible using the specified user account.

- The specified user account must have write permissions for at least one network share on the client, such as C$, Admin$ or a custom share. Access can be enabled by opening the **Network and Sharing center** and enabling **File and Printer Sharing** under **Advanced sharing settings** (Windows Vista and newer). On Windows XP, enable **File and Printer Sharing** on the **Exceptions** tab of Windows Firewall.

- When the client is not in a domain, additional settings must be configured:

  o **Simple File Sharing** (Windows XP) or the **Use Sharing Wizard** option (Windows Vista/ Windows Server 2008 or newer) must be disabled. It is enabled by default in all Windows installations and can be disabled by opening any folder in Windows Explorer, clicking **Organize** > **Folder and search options** > **View**, and unchecking the respective option.

  o When the client is using Windows Vista or newer: Open Registry Editor on the client and navigate to the key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion \Policies\System. Add a DWORD value named *LocalAccountTokenFilterPolicy* with value *1*.
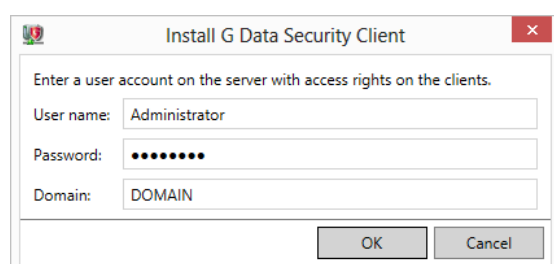
Using the **Server setup wizard**, which is automatically run the first time you start G DATA Administrator, you get an overview of all enabled computers in the network. You can also manually add and enable computers by name. Alternatively, the **Clients** module allows you to install G DATA Security 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, the **Installation overview** window is automatically opened. 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 **Security events** module if a reboot is required.

> 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.

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 installation medium to manually install the client software, or create a client installation package that can run in the background (which makes it ideal for distribution through logon scripts).

2.6.2.1. G DATA installation medium

Insert the G DATA installation medium and select **G DATA Security Client**.

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. Optionally, a group name can be entered. Once it connects to the ManagementServer, the client will be added to the corresponding group. See **Installation package** for more information about the rules for entering group names.

In order to prevent unauthorized access to the ManagementServer, clients that are deployed through a local installation need to be authorized in G DATA Administrator under **Clients** > **Overview** before they are fully served.

2.6.2.2. Installation package

The package is a single executable file (GDClientPck.exe), which can be used to install G DATA Security Client. 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 installation package for Windows clients**. You will be prompted for the following information:

- **ManagementServer**: The ManagementServer with which the clients should register.
- **Language**: The installation language.

- **Group**: The group to which the client will be added after the installation.

  Use a slash "/" to separate group names in a hierarchy. Special characters in group names must be marked: Every quotation mark in group names must be duplicated. If a group name contains a "/", the group name must be enclosed in quotation marks.

- **Limit validity**: Limit the validity of the installation package. If the package is installed after this period of time, it is considered unauthorized and needs to be manually authorized in G DATA Administrator under **Clients** > Overview.

Click **OK** and select a storage location. G DATA Administrator will create the installation package in the background. It can then be copied to the target computer and should be launched there with administrator rights in order to install G DATA Security Client. If the installation should be carried out without user interaction, start the installation package with the parameter /@_QuietInstallation="true": *GDClientPck.exe /@_QuietInstallation="true"*.

2.7. Installing G DATA Security Client for Linux

Like their Windows counterparts, Linux clients are managed by G DATA ManagementServer, allowing configuration via G DATA Administrator as well as automated virus signature update distribution. The basic client installation contains functionality for on-demand virus scans. Optionally, additional security modules for Linux servers can be installed.

The installation methods are similar to those of Windows clients: a remote installation via G DATA Administrator or a local installation using an installation script.

2.7.1. Remote installation

The most convenient way to install G DATA Security Client for Linux is to initiate a remote installation through G DATA Administrator. The prerequisites are as follows:

- The Linux machine must have an SSH server installed and running.
- The user account that is used to install the client must be able to log in to the SSH server using a password.
- DNS name resolution for the ManagementServer and the client must be available.
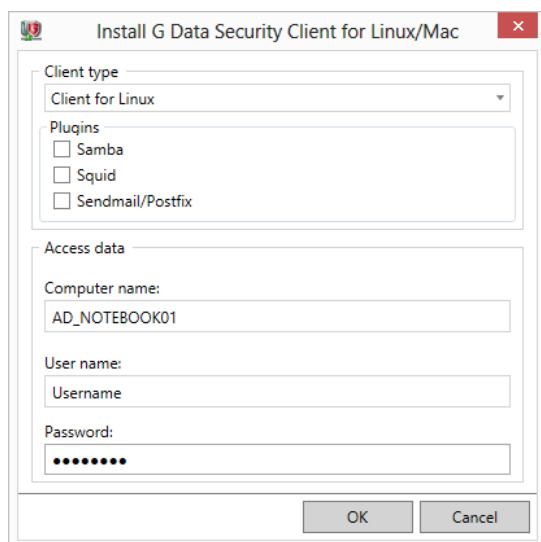
The installation is carried out as follows:

1. In the **Clients** module, select a Linux client, open the **Clients** menu and select the command **Install G DATA Security Client for Linux/Mac**.

2. Select the **Client type** (**Client for Linux**).

3. Optionally, select one or more **Plugins** (**Samba**, **Squid** oder **Sendmail/Postfix**). The prerequisites are described in the respective chapters.

4. Enter a **User name** and **Password**. The account must have root permissions.

5. Click the **OK** button. Installation progress will be shown in the **Installation overview** window.

2.7.2. Local installation

If a **remote installation** is not possible, you can install G DATA Security Client for Linux locally.

1. Start G DATA Administrator, select the **Clients** panel and choose the option **Create installation script for Linux/Mac clients** from the **Organization** menu.

2. After you choose a storage location, the script will be created in the background.

3. Copy the installation script to the client, then add the permission to execute the script (command-line: *chmod +x install-client.sh*).

4. Open a Terminal window and elevate the user status by typing *su* and entering the root password. Alternatively, execute the command from step 5 using *sudo*.

5. Navigate to the folder to which you copied the file and execute it: *./install-client.sh -t <product[,product]>*. The product parameter should be one or more of the following values:

   o *ALL*: G DATA Security Client for Linux and all additional modules

   o *WS*: G DATA Security Client for Linux

   o *SMB*: Samba module

   o *AMAVIS*: Sendmail/Postfix module

   o *WEB*: Squid module

6. In order to prevent unauthorized access to the ManagementServer, clients that are deployed through a local installation need to be authorized in G DATA Administrator under **Clients** > **Overview** before they are fully served.

2.7.3. Additional modules

G DATA Security Client for Linux contains additional modules that provide security to multiple Linux components. If you select additional modules during the remote or local installation, the modules are automatically installed. However, some modules need additional configuration before or after the installation.

2.7.3.1. Samba

After installing G DATA Security Client for Linux, Samba security can be enabled by adding the line *vfs objects = gdvfs* to the Samba configuration file (typically /etc/samba/smb.conf). To protect all shares, add it to the section *[global]*. If the line is in another section, the protection only applies to the corresponding share. After saving the configuration file, restart the Samba service.

2.7.3.2. Linux Mail Security Gateway

The Linux Mail Security Gateway module is available as an **optional module**.

The Linux Mail Security Gateway (Sendmail/Postfix) module has been developed as a plugin for the Amavis framework. Linux Mail Security Gateway requires Amavis 2.8.0 or higher and altermime. If Amavis is not available on the system, it will be automatically installed while installing the Linux Mail

Security Gateway module. The following configuration steps are required:

1. The Linux Mail Security Gateway module requires an operational Sendmail/Postfix mail server.
2. Make sure that the mail server forwards email messages to Amavis. More information can be found in the documentation of Amavis or the relevant mail server.
3. Make sure that spam and virus checks have been enabled in the Amavis configuration. More information can be found in the Amavis documentation.
4. Edit the configuration file /etc/gdata/amavis/mms.cfg and make sure that the mail server (sub) domain name has been entered under *localDomains* (e.g. *mail.domain.com*).

Using an existing Amavis installation is not recommended, because that requires a large number of changes to configuration files directly after installing the Linux Mail Security Gateway module.

Once configured, the Linux Mail Security Gateway module will automatically check email traffic and report viruses to G DATA ManagementServer. Its settings can be managed through G DATA Administrator in the **Sendmail/Postfix** module.

> Warning: When using an Amavis version older than 2.10.0, not all functions of the Linux Mail Security Gateway module are available. Update Amavis to version 2.10.0 or higher before deploying the Linux Mail Security Gateway module to ensure full functionality.

2.7.3.3. Linux Web Security Gateway

The Linux Web Security Gateway module is available as an **optional module**.

If you select the Linux Web Security Gateway (Squid) module, the installation of G DATA Security Client for Linux automatically installs and configures Squid itself. If Squid is already present on the system, the existing version will be uninstalled beforehand.

After the installation, the host name or IP address of the Squid server should be configured as proxy server on all systems for which traffic should be filtered by Squid (port 3128). To enable HTTPS traffic scans, additionally configure an HTTPS proxy with the Squid host name or IP address and port 6789. The required certificates are located in the /etc/gdata/ssl folder on the Squid server and should be imported on all clients. If you are using your own SSL certificates, they must be saved on the server in the folder /etc/gdata/ssl.

> Warning: The Squid server installation will use the package that is available in the respective distribution's repository. If that Squid version is older than 3.3.8, HTTPS scans will not be available.

Once enabled, the Linux Web Security Gateway module will automatically check traffic against a blacklist and report viruses to G DATA ManagementServer. Its settings can be managed through G DATA Administrator in the **Squid** module.

2.8. Installing G DATA Security Client for Mac

G DATA Security Client for Mac offers centrally managed malware protection and is managed by G DATA ManagementServer, allowing configuration via G DATA Administrator as well as automated virus signature update distribution.

The installation methods are similar to those of Windows and Linux clients: a **remote installation** via G DATA Administrator or a **local installation** using an installation script.

2.8.1. Remote installation

The most convenient way to install G DATA Security Client for Mac is to initiate a remote installation through G DATA Administrator. The **requirements** and the installation procedure are almost identical to the procedure for Linux:

1. In the **Clients** module, select a Mac client, open the **Clients** menu and select the command **Install G DATA Security Client for Linux/Mac**.
2. Under **Client type**, select **Client for Mac**.
3. Enter a **User name** and **Password**. The account must have root permissions.
4. Click the **OK** button. Installation progress will be shown in the **Installation overview** window.
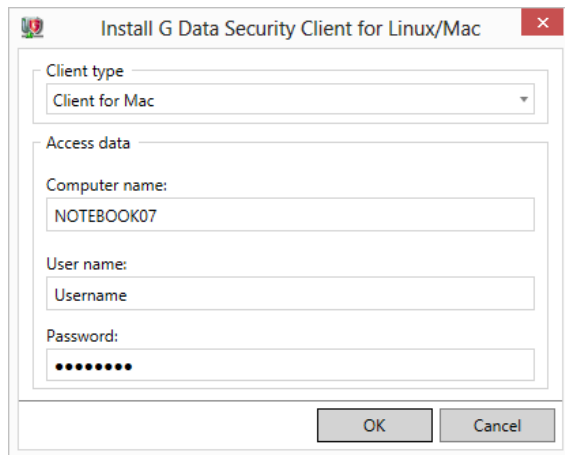
2.8.2. Local installation

If a **remote installation** is not possible, you can install G DATA Security Client for Mac locally.

1. Start G DATA Administrator, select the **Clients** panel and choose the option **Create installation script for Linux/Mac clients** from the **Organization** menu.
2. After you choose a storage location, the script will be created in the background.
3. Copy the installation script to the client.
4. Open a Terminal window and elevate the user status by typing *su* and entering the root password. Alternatively, execute the command from step 5 using *sudo*.
5. Navigate to the folder to which you copied the file and execute it: *./install-client.sh -t WS*.
6. In order to prevent unauthorized access to the ManagementServer, clients that are deployed through a local installation need to be authorized in G DATA Administrator under **Clients** > **Overview** before they are fully served.

2.9. Installing G DATA Exchange Mail Security/MailSecurity MailGateway

The deployment type of G DATA MailSecurity depends on the mail server that is used in the network. For networks that are using Microsoft Exchange Server 2007 SP1/2010/2013/2016, it can be installed as a plugin. Exchange Mail Security registers itself with ManagementServer and is administered by G DATA Administrator. The stand-alone gateway solution MailSecurity MailGateway can be used with all mail servers. It can be configured using G DATA MailSecurity Administrator, which will be installed alongside it.

2.9.1. Exchange Mail Security

The installation wizard of Exchange Mail Security adds a plugin to Microsoft Exchange Server 2007 SP1/2010/2013/2016. It should be installed on all Exchange servers that are running the Mailbox or Hub Transport roles.

To install G DATA Exchange Mail Security, insert the G DATA installation medium, select **G DATA MailSecurity for Exchange** and follow the installation wizard. The plugin reports to G DATA ManagementServer, which must have been installed beforehand. After installing the plugin, log in to the ManagementServer using G DATA Administrator to configure all protection settings on the **Exchange settings** tab.

In order to prevent unauthorized access to the ManagementServer, Exchange clients that are deployed through a local installation need to be authorized in G DATA Administrator under **Clients** > **Overview** before they are fully served.

2.9.2. MailSecurity MailGateway

MailSecurity MailGateway can be installed on a dedicated server or on the mail server itself. When installing MailSecurity MailGateway, several configurations are possible, depending on the PC in the network on which it will be installed. Ideally, it should 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.

To install MailSecurity MailGateway, insert the MailSecurity installation medium and press the **Install** button. Under **Mail Gateway**, select the **MailSecurity** component and follow the installation wizard. 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**.

Whichever deployment is chosen, several options (IP addresses, ports) should be configured directly after installing MailGateway, on the mail server as well as on the computer where MailGateway was installed. Example port configurations for various deployment scenarios can be found in the Reference Guide.

Depending on how your network is set up, MailGateway can use various nodes to check email for spam and virus infections:

- If you receive your email directly from an external POP3 server, MailGateway can be configured to check POP3 email messages for viruses before they are opened by the recipient. This can be set up under **Options** > **Incoming (POP3)**.

- If you are using a local SMTP server to receive e-mail, MailGateway can check incoming email even before it reaches the mail server. This can be set up under **Options** > **Incoming (SMTP)**.

- MailGateway can scan all your outgoing email for virus infections before sending anything to the recipient. This can be set up under **Options** > **Outgoing (SMTP)**.

2.10. 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 on your Android devices. G DATA Administrator offers installation capabilities for Android clients in the **Clients panel**. Select the clients and click **Send installation link to mobile clients** to send an e-mail containing a download link for the Internet

Security app.

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 for Android will be installed and can be started from the Android app menu.

To finalize the installation, remote administration has to be enabled. The e-mail contains a link that automatically opens G DATA Internet Security for Android and configures the relevant settings. Alternatively, enter the data manually. Open the **Settings** > **General** menu, 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 update server 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 all G DATA servers and clients in the network. G DATA Administrator is password-protected and can be installed on and launched from any Windows computer in the network.

After the first start, it is recommended to execute the **Server setup wizard** to walk through the most important settings of G DATA Administrator and G DATA ManagementServer and optimize them for your network.

4.1. Starting G DATA Administrator

Start G DATA Administrator by clicking the **G DATA Administrator** option in the program group **Start** > **(All) Programs** > **G DATA** > **G DATA Administrator**. In the following login screen, enter your login data:

- **Language**: Select the display language.
- **Server**: Enter the name of the computer on which G DATA ManagementServer was installed. To the right, a status indicator displays whether the ManagementServer is ready. If an error occurred, clicking the status indicator displays a log file.
- **Authentication**
  - **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 **Manage users**.
- **User name**: Enter your Windows administrator user name or your integrated authentication user name.
- **Password**: Enter your Windows administrator password or your integrated authentication password.
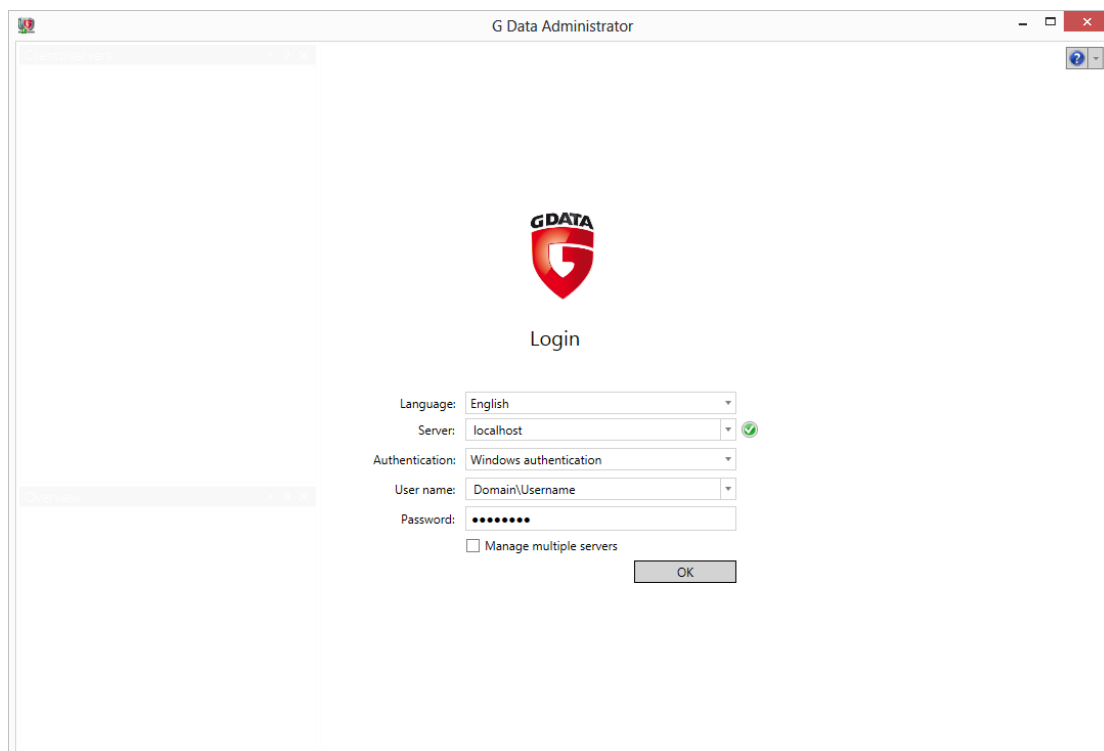
After entering your login data, click **OK** to log in.

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 relate to the use of Administrator, such as display options.

4.2. Using G DATA Administrator

The Administrator interface is organized as follows:
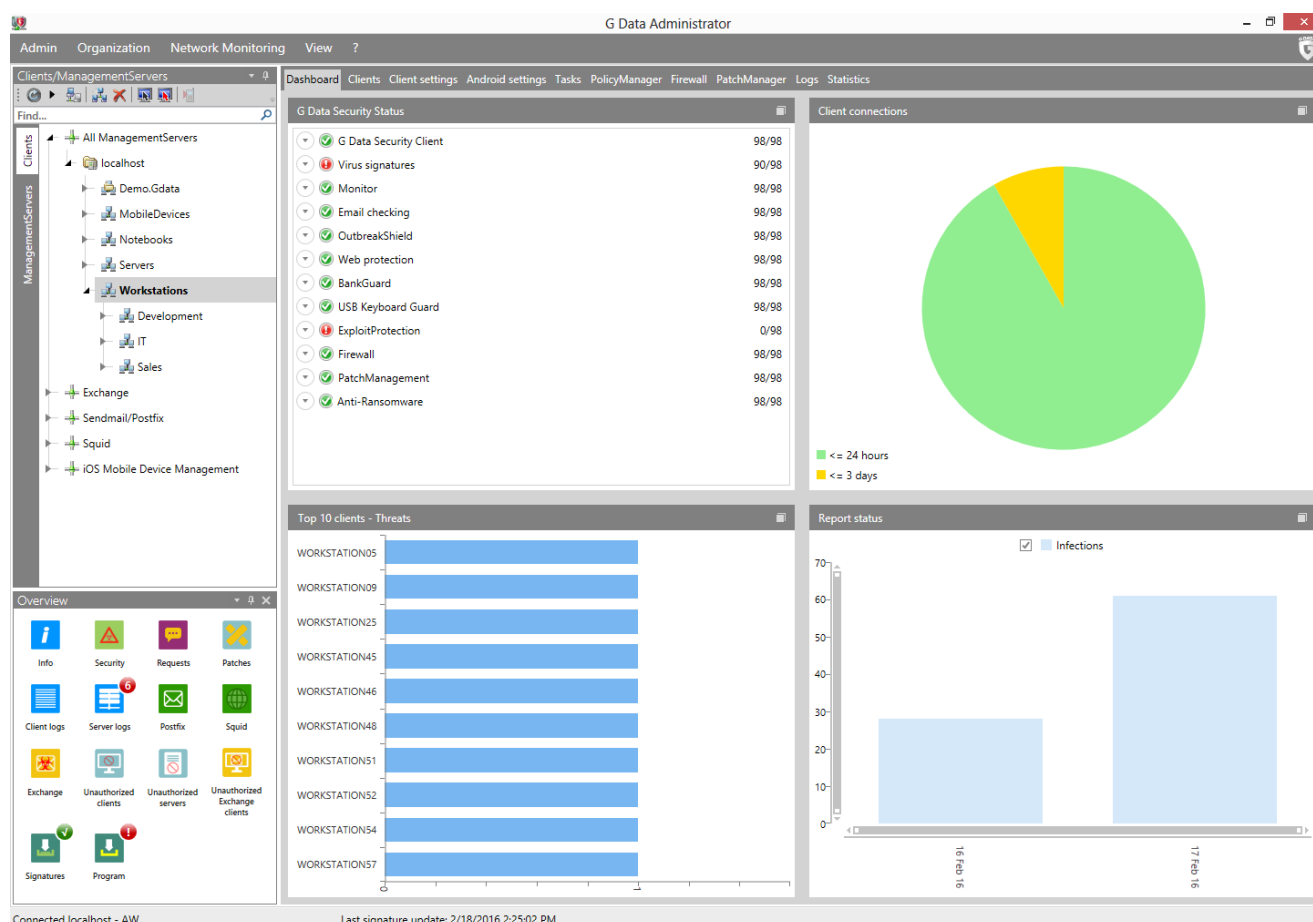
- The **Overview** panel offers global status information and shortcuts to items such as reports, logs and updates.

- The **Clients/ManagementServers** panel displays all clients and ManagementServers that can be managed.

- Configuration can be carried out using the **modules** that are accessible via dedicated tabs on the right. The availability of modules depends on the current selection in the **Clients/ ManagementServers** panel and on your **solution**.

- The menu bar offers access to global settings as well as additional menus that are only displayed when specific modules are selected:

  o **Admin**: Access to the **Server setup wizard** as well as exiting G DATA Administrator.

  o **Organization** (see **Clients/ManagementServers** > **Clients** > **Organization**)

  o **Clients** (see **Clients** > **Overview**)

  o **Tasks** (see **Tasks**)

  o **Firewall** (see **Firewall** > **Overview**)

  o **Security events** (see **Logs** > **Security events**)

  o **Network Monitoring**: Opens **G DATA ActionCenter** in order to use the optional Network

Monitoring **module**.

- o **View**: Show/hide the **Overview** panel.

- o **?**: Display the help file and version information.

4.2.1. Overview

The Overview panel displays an at-a-glance overview of unread reports, logs and other status information. Clicking the icons offers quick access to the respective modules with pre-configured filter settings to display only the requested data. The availability of icons depends on your G DATA **solution**.
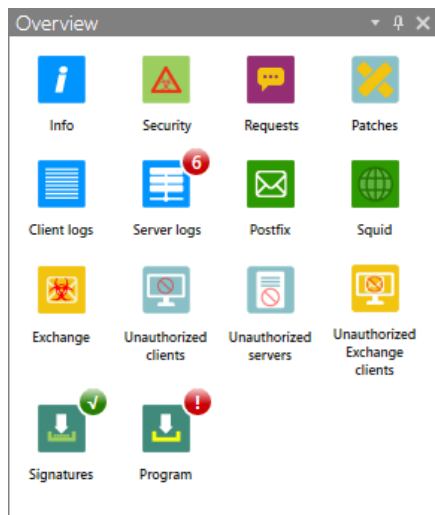
- **Info**: General information and error reports.

- **Security**: Infection reports.

- **Requests**: Requests from the PolicyManager, PatchManager and Firewall modules and from Android app control.

- **Patches**: High priority patches that have not yet been installed.

- **Client logs**: Client logs, such as changed settings and scan job status information.

- **Server logs**: ManagementServer information and error reports.

- **Postfix**: Sendmail/Postfix module reports.

- **Squid**: Squid module reports.

- **Exchange**: MailSecurity for Exchange reports.

- **Unauthorized clients**: Clients that have connected to the ManagementServer but have not yet been authorized by the administrator.

- **Unauthorized servers**: Subnet servers that have connected to the ManagementServer but have not yet been authorized by the administrator.

- **Unauthorized Exchange clients**: Exchange clients that have connected to the ManagementServer but have not yet been authorized by the administrator.

- **Signatures**: Version information for the virus signatures on the ManagementServer.

- **Program**: ManagementServer version information.

4.2.2. Clients/ManagementServers

The Clients/ManagementServers panel displays all clients and servers that are managed by G DATA Administrator. Select the **Clients** tab to display clients or the **ManagementServers** tab to display ManagementServers (primary servers, secondary servers and subnet servers).

Clients and ManagementServers are displayed in a node-based list. As in Windows Explorer, nodes that contain subordinated nodes appear with a small plus symbol. If you click on them, the structure expands and enables the view of the underlying nodes. Clicking the minus symbol collapses the list.

In the toolbar, you will see the most important client and server management commands, some of which are also displayed in the **Organization** menu. The availability of these options depends on the clients/ManagementServers that have been selected:

- **Refresh**
- **Expand/collapse all**: Expand or collapse all items in the network tree.
- **Show disabled clients**
- **Add group**
- **Delete**
- **Enable client**: Add a Windows or Linux client to the Clients tab by entering its name or IP address.
- **Installation overview**
- **Send installation link to mobile clients**: Send an installation link to Android and iOS clients.

4.2.2.1. Clients

The Clients tab lists the various types of clients under five top-level nodes:
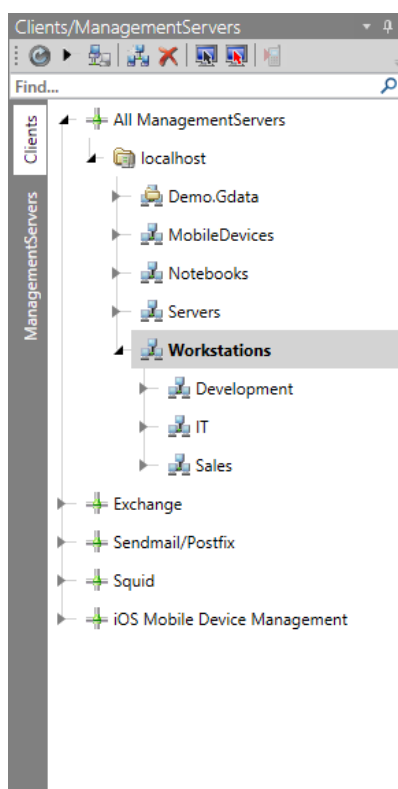
- **All ManagementServers**: Windows, Linux, Mac and Android clients.
- **Exchange**: Clients with the MailSecurity for Exchange plugin.

- **Sendmail/Postfix**: Linux clients with the Sendmail/Postfix module.
- **Squid**: Linux clients with the Squid module.
- **iOS Mobile Device Management**: iOS clients.

Before clients can be managed, they need to be added to the Clients tab and deployed. The procedure depends on the type of client, the network size and the configuration:

- Windows: Use the **Server setup wizard**, the **Find computer(s)** dialog window, the **Enable client** toolbar option or the **Active Directory support** to add Windows clients, then **deploy G DATA Security Client**.
- Linux: Use the **Enable client** toolbar option to add Linux clients, then **deploy G DATA Security Client for Linux**.
- Mac: Use the **Enable client** toolbar option to add Mac clients, then **deploy G DATA Security Client for Mac**.
- MailSecurity for Exchange: **Deploy G DATA MailSecurity for Exchange**. The Exchange client is then automatically added.
- Android: Use the **Send installation link to mobile clients** toolbar option to send an e-mail to the client. This initiates the **deployment of G DATA Internet Security for Android**. The Android client is then automatically added.
- iOS: Enter your login for G DATA ActionCenter in the **ActionCenter** module. Use the **Send installation link to mobile clients** toolbar option to send an e-mail to the client. After the end user has accepted the Device Management configuration, the iOS client is automatically added.

The following types of icons are shown on the Clients tab:

- Top-level node
- ManagementServer
- Group
- Group (Active Directory link)
- Client
- Client (disabled)
- Laptop client
- Mobile client
- Linux server
- Linux client
- MailSecurity for Exchange client
- Non-selectable devices: Devices like network printers fall under this category.

When a client, group or ManagementServer is selected, the corresponding **client modules** are displayed as tabs in the **module** area. Depending on the type of node you select, different modules are available. For example, when you select a desktop client, the tab **Client settings** will be enabled. For Android clients, on the other hand, you get access to the **Android settings** tab.

Client settings can be imported and exported. Right-click on a client and choose **Export settings** to export settings from the **Client settings** and **PolicyManager** modules to a .dbdat file. To import settings, select a client or group, choose **Import settings** and select the scope and the settings file.

Organization

When the Clients tab has been selected, the **Organization** menu is displayed in the menu bar, offering access to settings related to client organization.

Refresh

The Refresh function updates the list in the Clients/ManagementServers panel.

Show disabled clients

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

Add 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 ManagementServer or group, and then click the **Add group** option. After entering a group name, clients can be assigned to the new group by dragging and dropping them onto it.
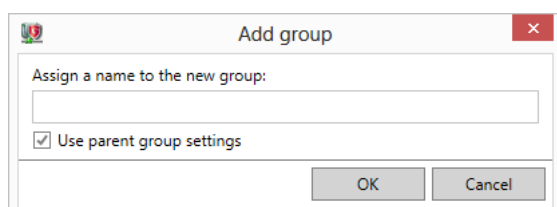
To move a large number of clients into a group, use the **Clients** > Overview module. Select the clients that should be moved, right-click and choose **Move clients**.

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 has been selected on the Clients tab.
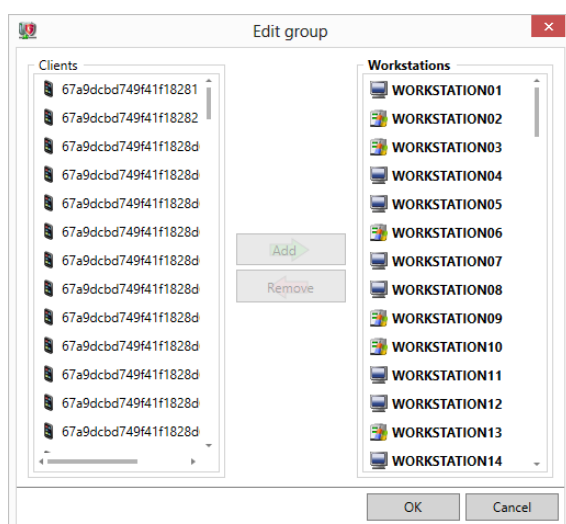
Delete

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.

Find computer(s)

The Find computer(s) window can be used to add clients to the Clients tab and enable them. Clients can be found by IP address and enabled directly from within the dialog window.
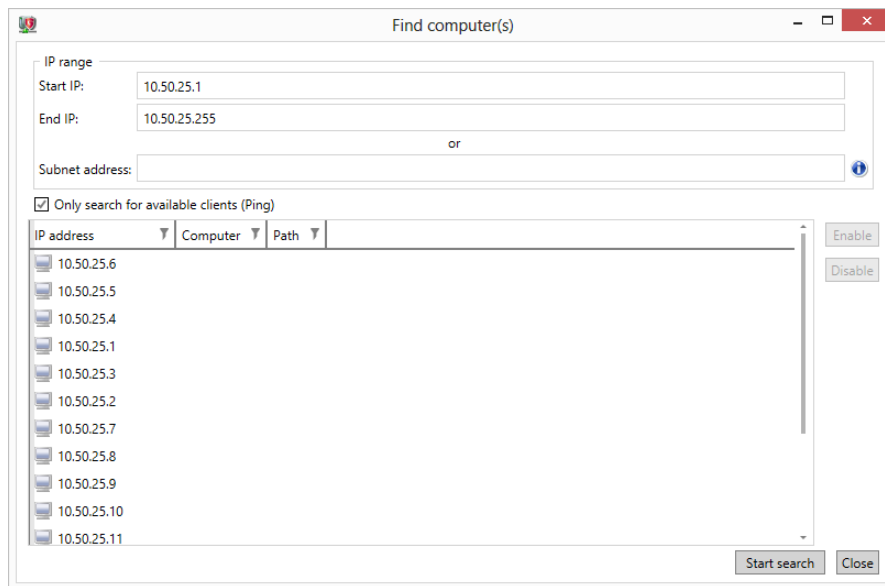
The Find computer(s) window will contact all computers in a specified IP range. The range can be defined using a **Start IP** and **End IP** (such as 192.168.0.1 and 192.168.0.255), or a **Subnet address** (in CIDR notation, such as 192.168.0.0/24). To make sure that only available clients are listed, 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 Clients tab. The search result includes enabled clients, if applicable - these can be disabled by clicking **Disable**.

Rule wizard

When clients connect to ManagementServer for the first time, they are automatically added to the group **New clients** if no group has been defined when enabling the client or creating the installation package. The Rule wizard can be used to create rules that regularly move new clients to predefined groups.

Rules can be managed using the **New**, **Edit** and **Delete** buttons and the arrow buttons next to the rule list. The **Import** and **Export** buttons can be used to import/export the rules as .json files.

Under **Settings**, the general settings for the execution of the rules can be defined:

- **Schedule**: The rules are executed **Hourly**, **Daily** or **Weekly**.
- **Time**: Define the exact point of time at which the rules are executed.
- **Apply group settings**: After being moved, clients are automatically assigned the settings from the group to which they were moved.
- **Only move clients from the group "New clients"**: The rules only apply to clients from the group **New clients**. If this option is deselected, the rules apply to all clients. This can cause clients to be moved around multiple times and should usually be left selected.
- **Execute now**: Execute the rules immediately.
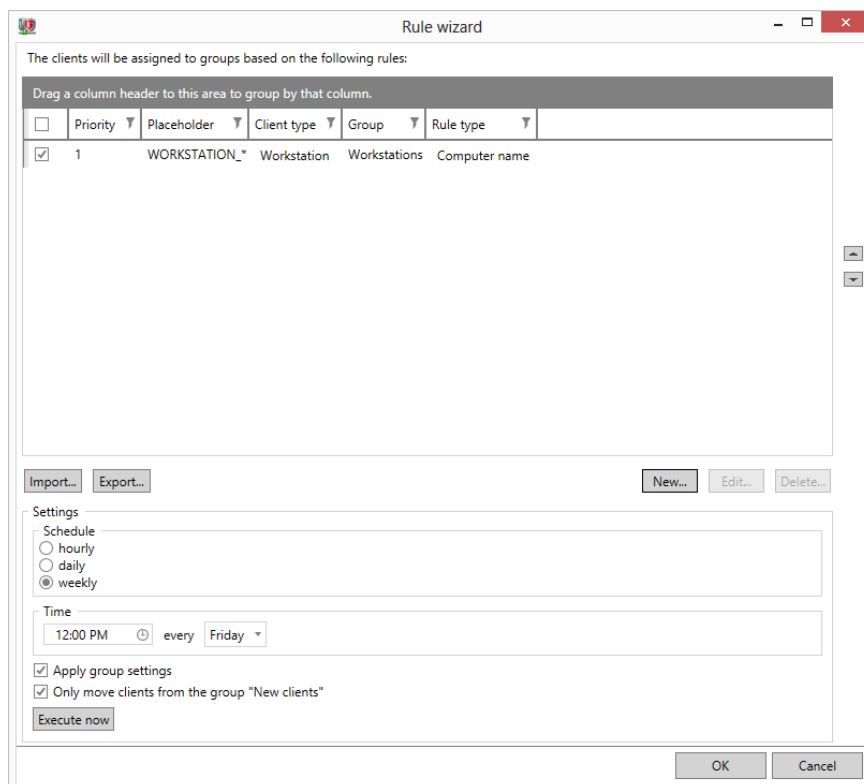
Using a number of settings, you can define rules that automatically move clients between groups:

- **Rule type**: Select whether the clients are selected by **Computer name**, **IP address**, **Domain** or **Default gateway**.

- **Client placeholder**: Enter the search string that is used to select clients. You can use placeholders. For example, enter *Sales_** to select all clients with the name prefix Sales_ (when using the **Computer name** setting) or *192.168.0.[1-100]* to select all clients with IP addresses between 192.168.0.1 and 192.168.0.100 (when using the **IP address** setting).

- **Client type**: Select which client types are moved (**All**, **Workstation**, **Server**, **Android device** or **Laptop**).

- **Groups**: Enter one or more groups or select them by double-clicking on a group in the tree view. When multiple groups have been entered, the selected clients will be divided equally over the groups.
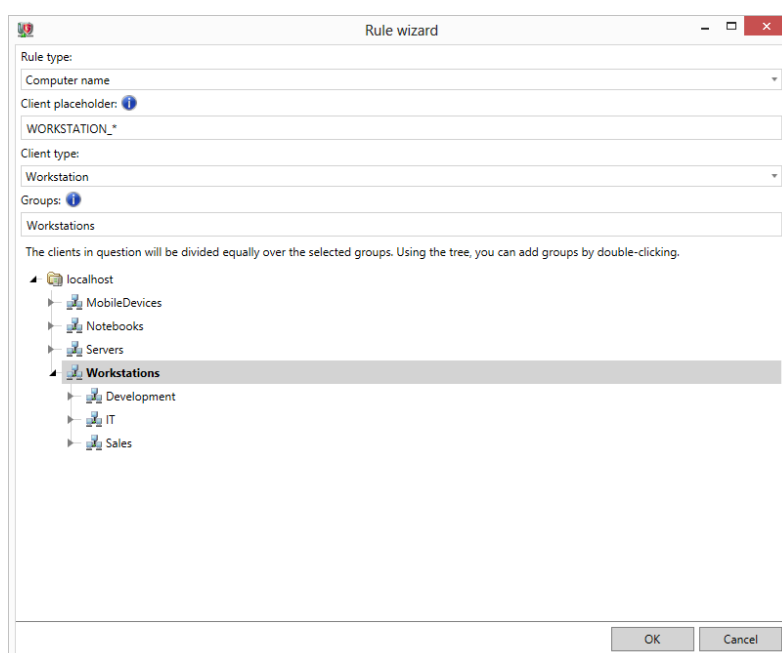
Create installation package for Windows clients
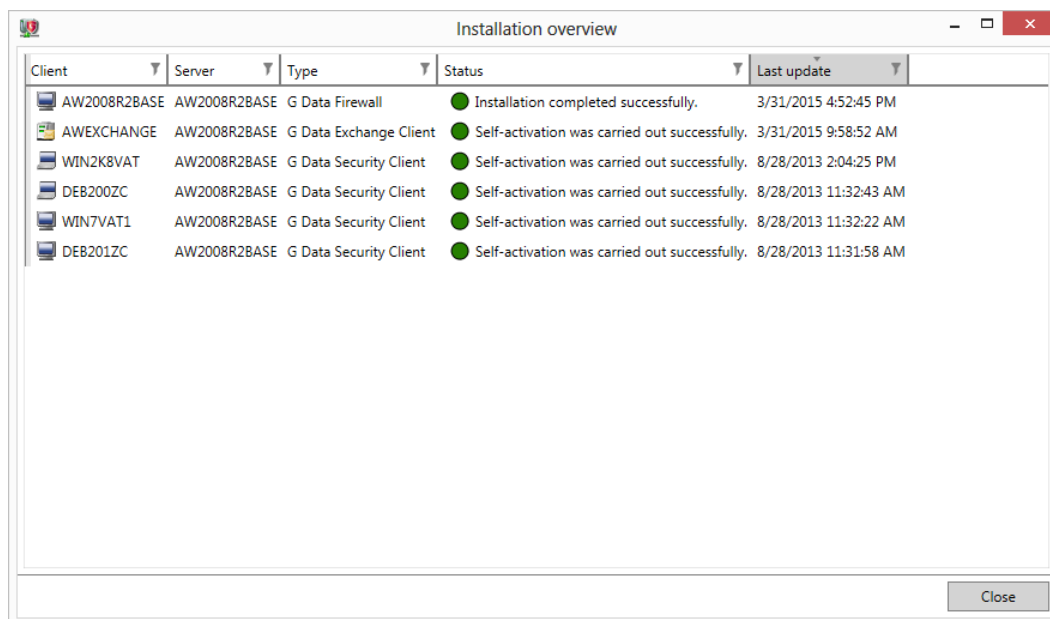
This function can be used to create an installation package for G DATA Security Client. Use the package to install G DATA Security Client locally. See the chapter **Installation package** for more details.

Create installation script for Linux/Mac clients

This function can be used to create an installation script for G DATA Security Client for Linux and G DATA Security Client for Mac. Use the script to install G DATA Security Client locally. See the chapters **Local installation (Linux)** and **Local installation (Mac)** for more details.

Installation overview

The Installation overview window can be used to keep track of installation progress. It opens automatically when a remote installation task is added, or can be opened by clicking the Installation overview button in the Clients/ManagementServers panel's toolbar.

Client	Server	Type	Status	Last update
AW2008R2BASE	AW2008R2BASE	G Data Firewall	● Installation completed successfully.	3/31/2015 4:52:45 PM
AWEXCHANGE	AW2008R2BASE	G Data Exchange Client	● Self-activation was carried out successfully.	3/31/2015 9:58:52 AM
WIN2K8VAT	AW2008R2BASE	G Data Security Client	● Self-activation was carried out successfully.	8/28/2013 2:04:25 PM
DEB200ZC	AW2008R2BASE	G Data Security Client	● Self-activation was carried out successfully.	8/28/2013 11:32:43 AM
WIN7VAT1	AW2008R2BASE	G Data Security Client	● Self-activation was carried out successfully.	8/28/2013 11:32:22 AM
DEB201ZC	AW2008R2BASE	G Data Security Client	● Self-activation was carried out successfully.	8/28/2013 11:31:58 AM

The Installation overview window lists all clients that have pending and completed remote installation tasks. The **Type** column shows the type of installation (for example G DATA Security Client; G DATA Internet Security for Android; Subnet server). After a remote installation has been completed, the **Status** column will be updated. For clients that have been added via **Active Directory synchronization**, the **Next installation attempt** column shows the time at which the remote installation will be started.

Right-clicking an entry offers the following options:

- **Refresh**: Refresh the list.
- **Delete entry**: Remove the selected entry from the list.
- **Show installation log**: Show the installation log for the selected entry.
- **Try again**: Retry a failed installation attempt.

Send installation link to mobile clients

The window **Send installation link to mobile clients** lets you send an installation e-mail to mobile clients. Depending on the selection on the Clients tab, the window will contain options for **Android** or **iOS** clients.

Opening the e-mail on the mobile client lets users **install G DATA Internet Security for Android**

(when deploying Android clients) or enable Device Management (when deploying iOS clients). After completing the respective procedure, the mobile client(s) will show up on the Clients tab.

> In order to send mobile clients an installation link, G DATA ManagementServer needs to be able to send e-mails. Make sure to enter your login data for an SMTP server under **General settings** > **Email > Email settings**.

Android clients
In order to send an installation link to Android clients, the following information should be entered:

- **Password**: If you have not yet entered a mobile authentication password under **General settings** > **Android** > **Authentication for mobile clients**, enter it here.
- **Recipient(s)**: Enter one or more e-mail addresses, separated by line breaks or commas.
- **Subject**: Enter the subject of the installation email.
- **Content**: Enter the body text of the installation email. It must contain the preconfigured placeholders for installation links.

Click **OK** to send the installation link.

iOS clients
When deploying Device Management to iOS clients, several settings allow you to customize the appearance of the Device Management request to the end user:

- **Name**: Enter the Device Management name.
- **Description**: Enter the Device Management description.
- **Organisation**: Enter your organization's name.
- **End User License Agreement**: Enter an End User License Agreement.
- **Recipient(s)**: Enter one or more e-mail addresses, separated by line breaks or commas.

Click **OK** to send the installation link.

> Before sending an installation link to an iOS client, make sure you have entered your ActionCenter login data in the **ActionCenter** module.

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, select **Assign to AD group** and choose 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. Enter **User name** and **Password** for a domain account with sufficient permissions on clients, as well as the installation **Language**.

By default, G DATA ManagementServer synchronizes its data with the Active Directory server every six hours. This value can be changed under **General settings** > **Synchronization**.

> Active Directory changes are automatically synchronized with Management Server. However, if clients are moved between domains, the Active Directory link of the Management Server group for the previous domain must be manually unassigned. After assigning an Active Directory item from the new domain to a Management Server group, the clients will then be automatically synchronized to the appropriate node on the **Clients** tab.

4.2.2.2. ManagementServers

The following types of ManagementServers are shown in the ManagementServers view:

- Top-level node
- Primary server
- Secondary server
- Subnet server
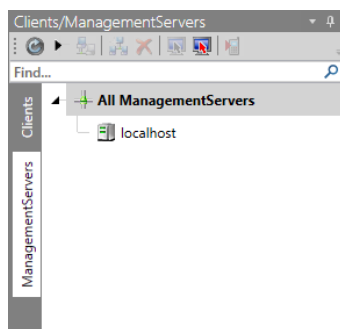
When a server is selected, the corresponding **server modules** are displayed as tabs in the **module** area.

4.2.3. Modules

Depending on the current selection in the **Clients/ManagementServers** panel, either the **client modules** or the **server modules** are shown as tabs on the right side of the window. Click any tab to open the corresponding module.

Most modules have a toolbar. In addition to module-specific functions, the following buttons are usually displayed:

- **Refresh**: Refresh the current list or view.
- **Delete**: Delete the currently selected item(s).
- **Print**: Print (selected) items from the current module.
- **Print preview**: Display a print preview.
- **Time frame**: Limit the displayed items to a specific time frame.

For most modules, there are also general options to control layout and list contents:

- To sort a list, click any of its column headers.
- To add or remove columns from the list display, right-click any column header, click **Select columns** and then (de)select the columns that should be displayed.
- To reduce the number 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.
- 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.

Each module's settings always apply to the clients, servers or groups highlighted in the **Clients/ ManagementServers** panel. If a ManagementServer or group has been selected, clients or groups within the group may have different values set for one or more settings. The affected settings will be marked as such. When saving the settings, each client with deviating settings will retain its own value. Only if the value is changed will it be applied to the whole group. Subordinated clients or groups that have settings that deviate from the group settings are displayed by name in the panel **Clients/groups with deviating settings**. Select a client and click **Display settings** to select that specific client in the **Clients/ManagementServers** panel and display its settings or click **Revert to group settings** to apply the group settings to that client.

When administering a group that contains Windows clients as well as Linux or Mac clients, settings

that have no effect on Linux or Mac clients are displayed in green.

Settings are only saved and transferred to the selected client(s)/server once the **Apply** button has been clicked. At the bottom of most modules, the **Information** status field shows whether the settings have been successfully transferred. Click the **Discard** button to discard the changes.

4.3. Client modules

The client modules can be used to configure the (groups of) clients that have been selected on the **Clients** tab of the **Clients/ManagementServers** panel.

4.3.1. 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 **Clients** panel 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 has possible security problems (e.g. the monitor is switched off or a client's virus signatures are out of date), a warning symbol will alert you.
- ℹ️ When the G DATA program interface opens, some settings may be displayed in info mode for a short time. This does not mean that the network is not protected at that time: G DATA ManagementServer's database is simply 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.
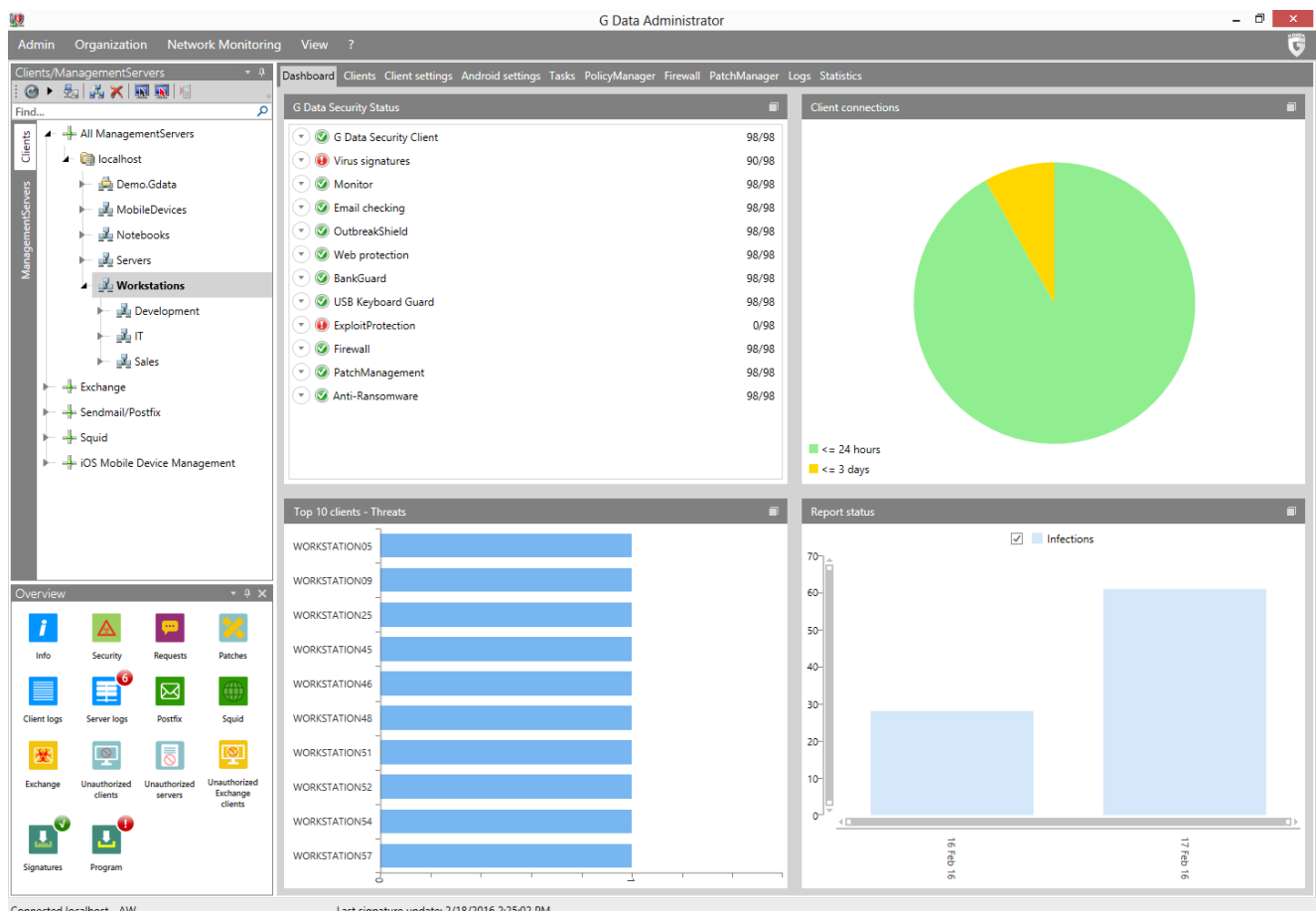
The **Client connections** chart offers an overview of the connections that have been made to G DATA ManagementServer. Using the chart you can make sure that all clients are regularly connecting to G DATA ManagementServer. The clients that appear under **Top 10 clients - Threats** should be monitored 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 **G DATA Endpoint Protection Business**) might be advisable. **Report status** offers visual representation of the number of infections, queries, and errors in your network.

4.3.2. Clients

The Clients module offers 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.

4.3.2.1. Overview

From the Overview panel, you obtain an overview of all managed clients and can also simultaneously carry out any client administration. Using the **Security status** column, you can easily keep track of every client's current security status.

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

- **Refresh**
- **Delete**: Remove a client from the Clients list. As this option does not uninstall G DATA Security Client from the client, it should only be used for client machines that have already been decommissioned or removed from the network. If an active client is inadvertently removed from the list, it will reappear upon its next connection to ManagementServer (group-specific settings, however, are lost).

- **Print**

- **Print preview**

- **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. The **Clients** menu and the right-click context menu offer the following functions:

- **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 the selected client(s) to the group settings.

- **Move clients**: This function allows you to move the selected client(s) to an existing group. After selecting this function, a dialog window displays all existing groups. 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 Android clients).

- **Remove assigned EULA**: Removes an assigned EULA from the selected client(s) (only available for Android clients).

- **EULA management**

- **Assign G DATA server**: While you have the option of assigning specific subnet servers to clients with the function **Servers** > **Overview**, 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:
  - **Open message box on client**: Inform the user that they should restart his/her client computer at a convenient time.
  - **Create report**: Create a report in the **Security events** module.
  - **Force reboot**: Automatically force a restart.

- **Delete** (only in the context menu)

- **Authorize** (only in the context menu): Authorize the selected client(s). In order to prevent unauthorized access to the ManagementServer, clients that are deployed through a local installation need to be authorized before they are fully served.

- **Properties** (only in the context menu): Display properties for the selected client (**General**, **Network info**, **Security risks** and **Hardware**).

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 displays the disabled clients.

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

Uninstall G DATA Security Client

Using the uninstall function, G DATA Security Client (for Windows and Linux) 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.
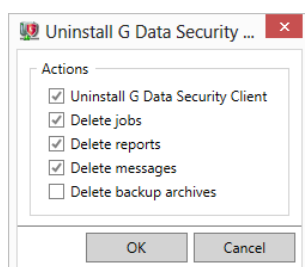

Alternatively, it is possible to uninstall the client locally. This requires administrator rights. In the folder %ProgramData%\G Data\client, start setup.exe to start the uninstallation. The computer should be restarted afterwards. For Linux clients, use the gdata_uninstall.sh script, which is typically located at /usr/sbin/gdata_uninstall.sh.

Manage EULAs

The Manage EULAs window allows you to add, edit and remove End User License Agreements (EULAs) for Android devices. Using the appropriate options in the Clients menu, these EULAs can then be assigned to any Android device to make sure the end user is informed about and has agreed with the deployment of G DATA's Internet Security for Android 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**.
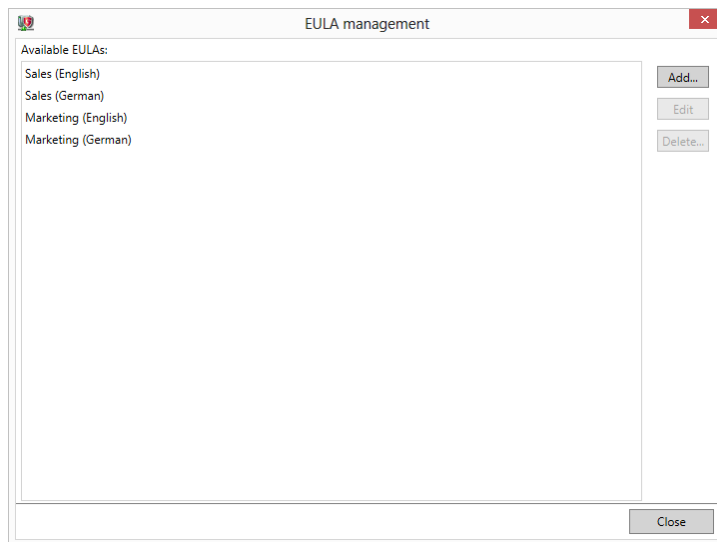
4.3.2.2. Software

The software inventory allows you to monitor software use across the whole network. Software can be added to a blacklist or whitelist to support software management in the network.
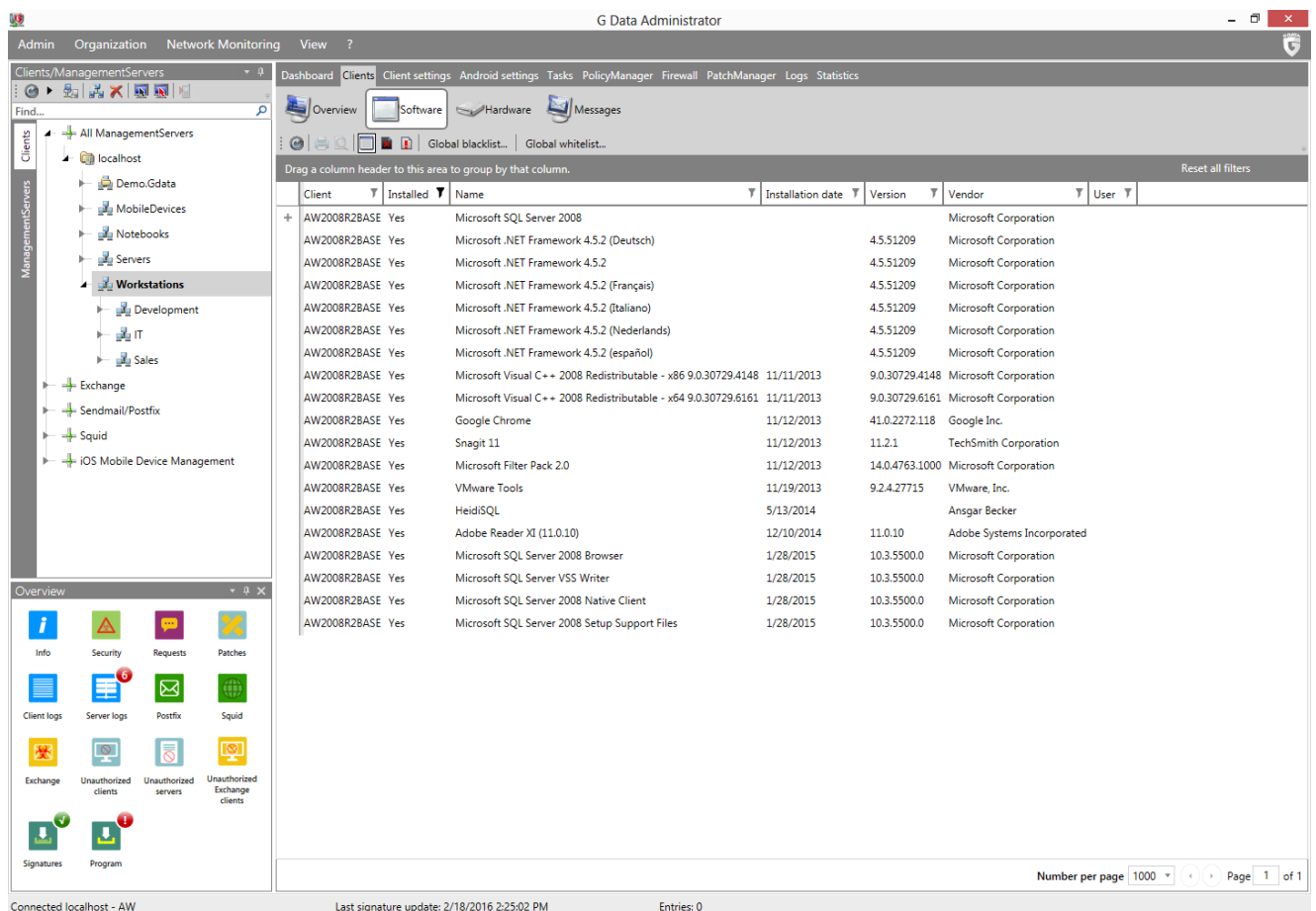
The software overview can be managed with the following toolbar buttons:

Refresh

Print

Print preview

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

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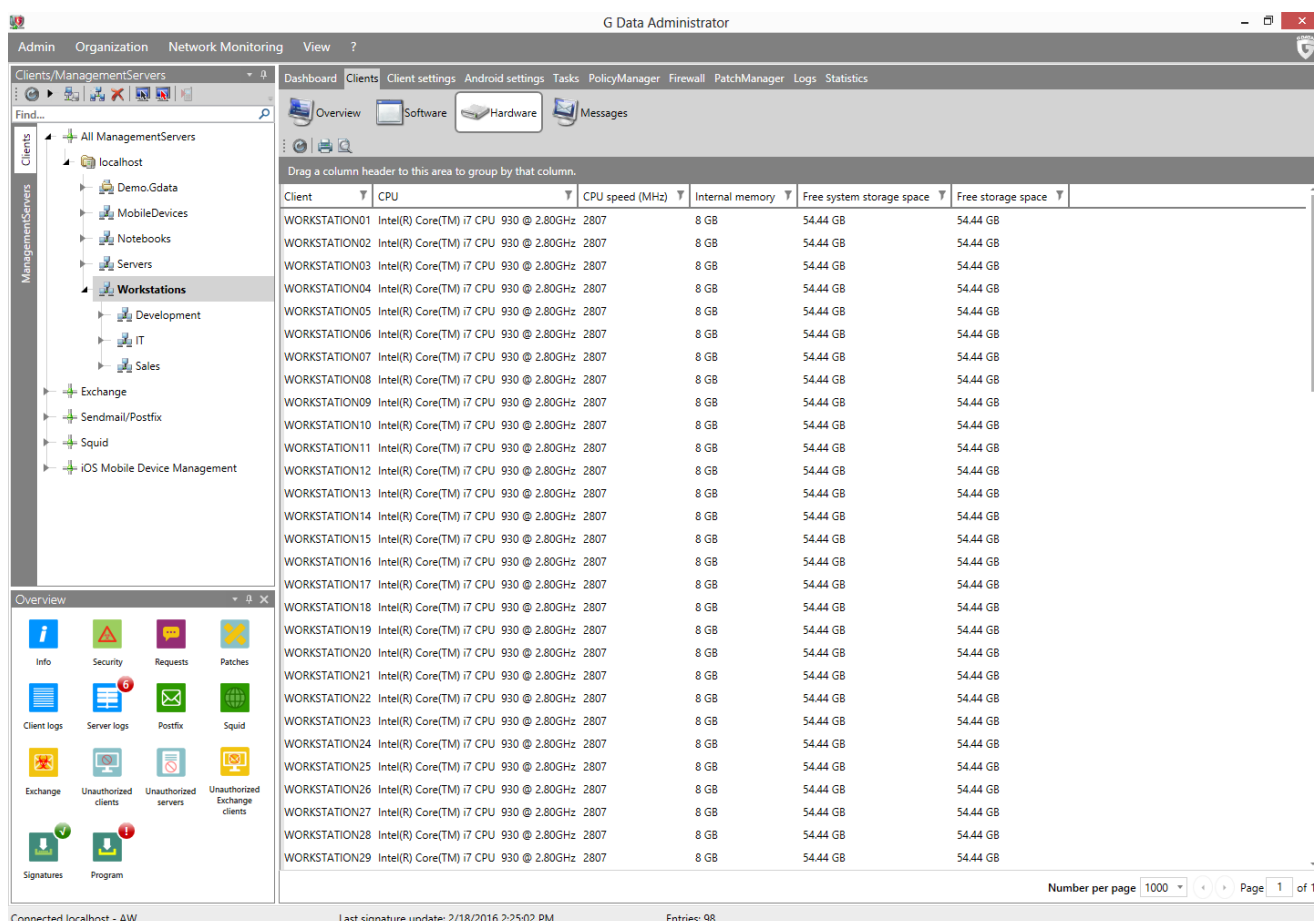
⚠️ **Display only software that is not on the whitelist**: Only show software that is installed on the network clients, but has not been checked yet by the system administrator. Using this view, you can quickly add software to the blacklist or whitelist by right clicking on it.

The list area lists installed software for all clients selected in the **Clients panel**. To fill the blacklist or whitelist, click the button **Global blacklist** or **Global whitelist**. Click **Add** to add a new blacklist or whitelist entry. 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.

By default, the Software inventory is filtered to only show currently installed applications. To show all applications, including those that were previously installed but are no longer present, click **Reset all filters** to reset the display filter.

4.3.2.3. Hardware

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

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

- 🔄 **Refresh**
- 🖨️ **Print**
- 🔍 **Print preview**

4.3.2.4. Messages

You can send messages to individual clients or client groups to quickly and conveniently inform users. The messages are displayed as a small popup on the bottom right of the client desktop.
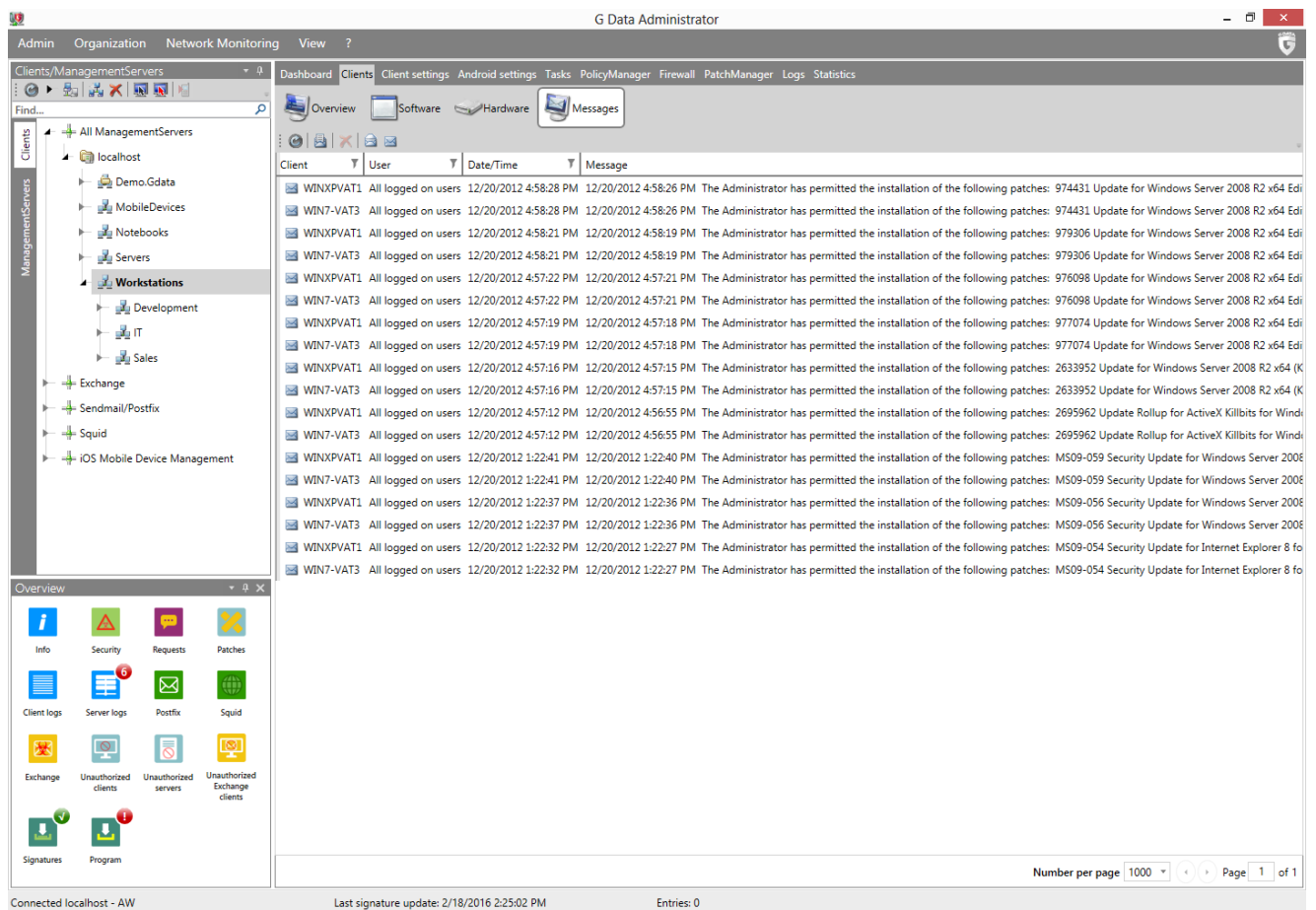
To create a message, simply click the **Send message** button. In the dialogue window, select the clients you want to send the message to. If you want a message to be sent only to a specific end user on the selected client(s), enter their **User name**. Type your information in the **Message** field and click the **OK** button.

4.3.3. Clients (iOS)

When you have selected one or more iOS clients in the **Clients** panel, the Clients module only displays details pertaining to the selected iOS client(s):

- **Client**: Device name.
- **Security status**: Shows the current security status and displays a warning if no **profile** has been assigned or if the profile is pending.
- **Profile**: Displays the currently assigned **profile**. Select a profile from the list to change the profile or select **- No profile -** to remove the current profile.
- **Last access**: Timestamp for the most recent connection between the iOS client and G DATA ActionCenter.
- **IMEI**: Device IMEI identification number.
- **Capacity**: Device storage capacity in GB.
- **Version**: iOS version number.
- **Telephone number**: Device telephone number.

- **Email address**: The email address to which the installation link was sent.
- **Product name**: Device product name.
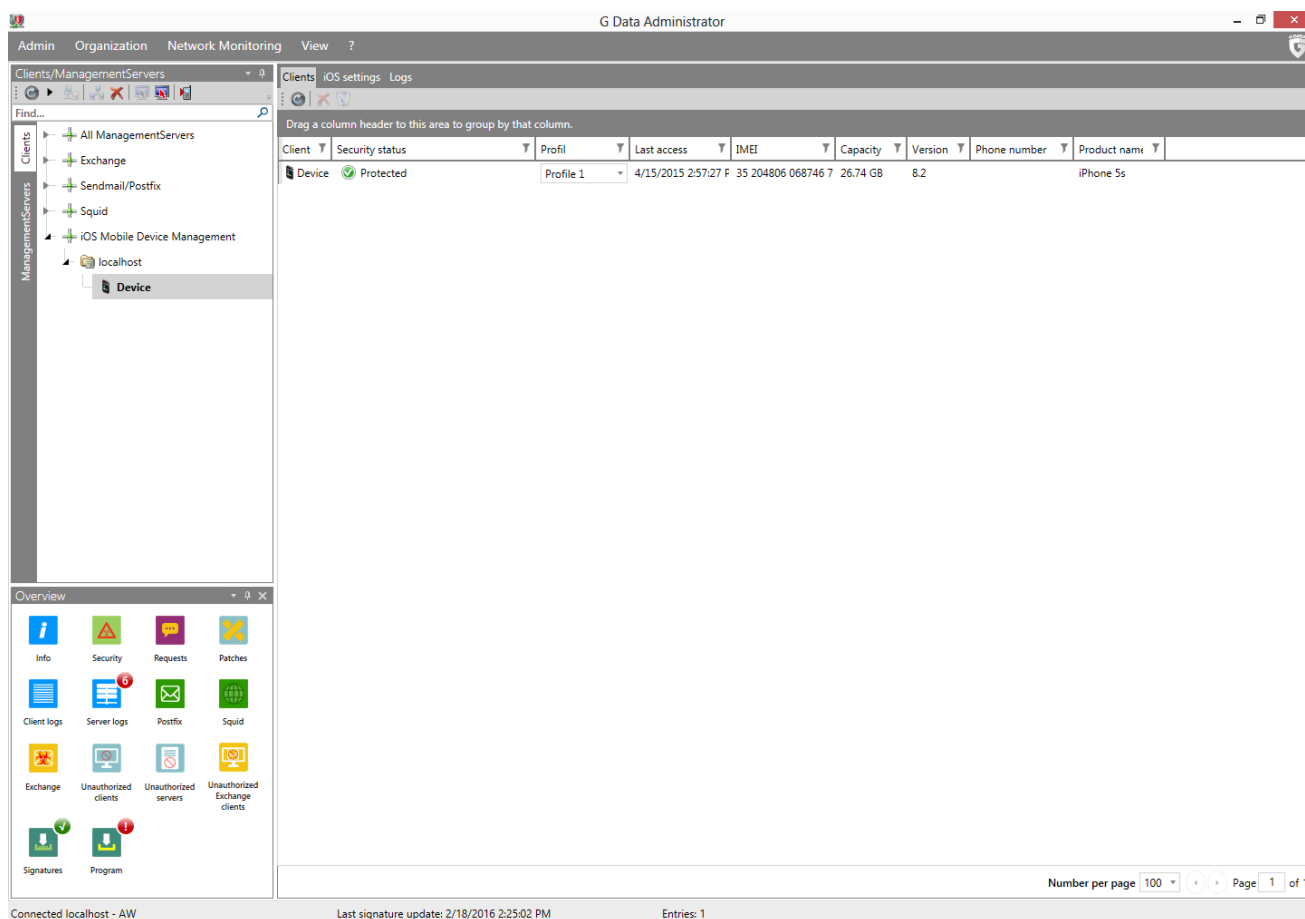
Right-click a client to select one of the following context options:

- **Delete device management**: Disable mobile device management on the device.
- **Delete**: Remove the device from the list. Before removing the device from the list, use **Delete device management** to disable mobile device management.
- **Resend activation email**: Resend the installation link to clients with an inactive or pending MDM installation.

4.3.4. Client settings

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

4.3.4.1. General

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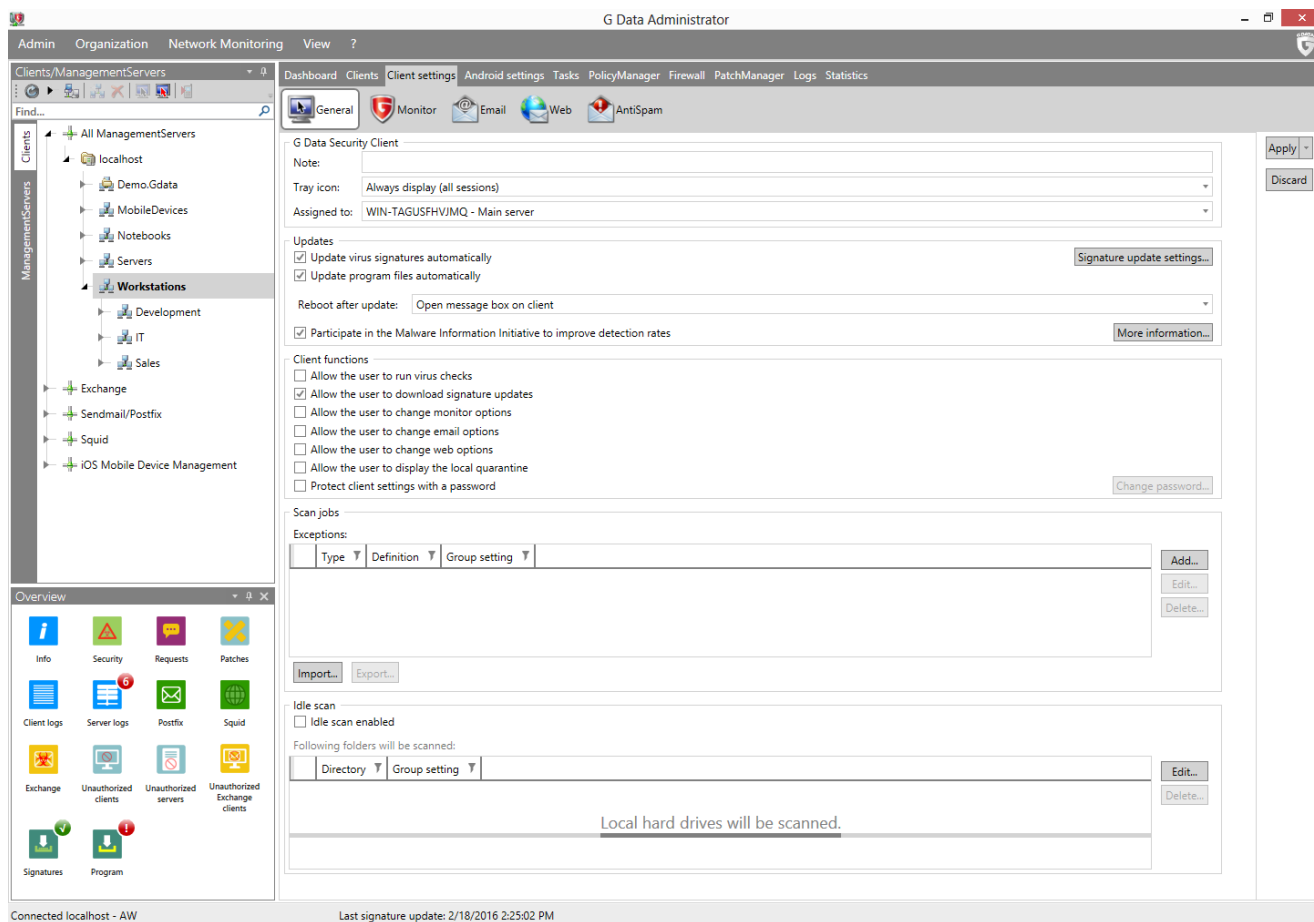
G DATA Security Client

The G DATA Security Client section covers basic client functionality.

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

- **Tray icon**: Choose when the client icon should be displayed in the system tray: **Never**, **Display in first session only** (for terminal servers and Windows Fast user switching) or **Always display (in all sessions)**. If the icon is not displayed, the functionality of Security Client is severely limited (for example, Idle scan cannot be used and the user has no access to the Client functions).

- **Assigned to**: By default, clients are assigned to the main ManagementServer. The dropdown list displays the main ManagementServer and its subnet servers and can be used to quickly assign a client to a specific (subnet) server.

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. At every synchronization interval the clients 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. At every synchronization interval the clients 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 Security events module, or select **Force reboot** to automatically force a restart.

- **Participate in the Malware Information Initiative to improve detection rates**: Enable participation in the Malware Information Initiative. The G DATA SecurityLabs continuously research new technologies to protect our customers against malware (viruses, worms and malicious programs). The more information is available, the higher the efficacy of the technologies. However, much information is available only on systems that have been attacked or infected. In order to include even such information in the analyses, the G DATA Malware Information Initiative was founded. In this context, malware-related information is sent to the G DATA SecurityLabs.

- **Signature update settings**: Define where clients obtain their virus signature updates:

  o **Load signature updates from the ManagementServer**: Clients will obtain virus signature updates from their ManagementServer. They will check for updates at every synchronization interval.

  o **Load online signature updates independently**: Clients will obtain updates from the central G DATA update servers. The update check can be scheduled under **Settings and scheduling**.

  o **Load online signature updates independently, if no connection to the ManagementServer can be established**: This option is recommended for mobile workstations such as laptops. When the client has a connection to the ManagementServer, it will download its updates from there. If there is no connection to the ManagementServer, the virus signatures are automatically downloaded from the G DATA update servers. The update check can be scheduled under **Settings and scheduling**.

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 options**: If this function is enabled, the client user has the option to change the Web 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. 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 end users from changing 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.

Idle scan

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

4.3.4.2. 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.
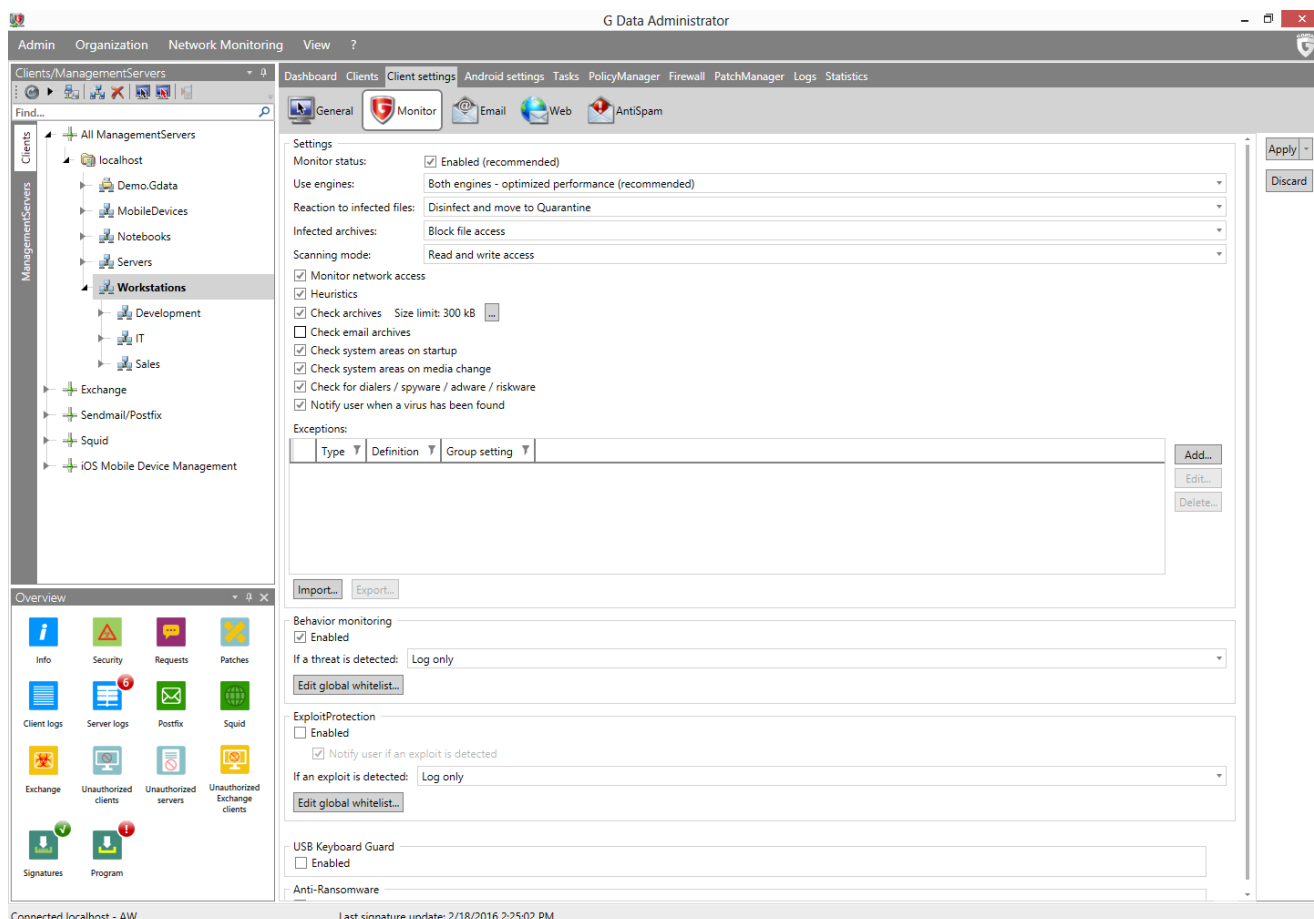
Settings

Monitor settings can be used to configure the monitor 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 can have performance advantages.

- **Reaction to infected files**: Specify the action to be taken if an infected file is detected. There are various options that may or may not be suitable, depending on what the respective client is used for:

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

  - **Disinfect and move to quarantine**: The file is moved to quarantine and an attempt is made to remove the virus.

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

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

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

- **Scanning mode**: Define when files should be scanned. **Read access** scans every file directly when it's read. **Read and write access** adds a scan on writing, to protect against viruses that are copied from another possibly unprotected client or from the Internet. **On execution** scans files only when they are executed.

- **Monitor network access**: Enable network access monitoring.

- **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**/**Check system areas on media change**: System areas (such as 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 checks, 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:

- **Directory**: Select a folder (including any subfolder contained within it) that you do not want to be checked by the monitor.

- **Drive**: Select a drive (partition, hard disk) 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 use wildcards.

    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. .xls, .xlsx), simply enter *.xls?. 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.

- **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.

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.

Whenever behavior monitoring carries out an action, a report is added to the Security events tab. If a program has falsely been identified as a threat, the corresponding report can be used to create a whitelist entry. Whitelist entries can be viewed and removed by clicking **Edit global whitelist**.

ExploitProtection

Exploits specifically look for vulnerabilities in third party software on the client. ExploitProtection constantly checks the behavior of the installed software for irregularities. If any unusual behavior is detected in a software process, the action that has been defined under **If an exploit is detected** is carried out: **Log only** or **Prevent execution**. If **Notify user if an exploit is detected** has been enabled, the user will also receive a notification.

Whenever ExploitProtection carries out an action, a report is added to the Security events tab. If a program has falsely been identified as a threat, the corresponding report can be used to create a whitelist entry. Whitelist entries can be viewed and removed by clicking **Edit global whitelist**.

USB Keyboard Guard

USB Keyboard Guard protects clients against BadUSB attacks. Maliciously reprogrammed USB devices, such as cameras, USB sticks or printers, can act as keyboards when they are plugged in to a computer. To prevent those devices from automatically carrying out unauthorized commands, USB Keyboard Guard will ask the user for confirmation if it detects a USB device that identifies itself as a keyboard. If the user indeed plugged in a keyboard, it can be safely authorized. If the device identifies itself as a keyboard but the user plugged in something else, it should not be authorized, as it may be malicious.

Regardless of the user's decision, a report will be added to the Security events tab. If a device has been authorized, the administrator can decide to block it nonetheless by right-clicking on the report and revoking the authorization.

Anti-Ransomware

Whereas regular malware infects devices to use them as part of a botnet or to steal credit card information, ransomware developers try to make money by extorting the user directly. In order to extract a ransom, ransomware locks the device or even encrypts data until the victim pays up. In addition to signature- and behavior-based detection, the Anti-Ransomware function detects the specific actions of ransomware, such as file encryption, and blocks them before it can do any more harm. When ransomware is detected, the action set under **In case of a threat** will be carried out. The options **Log only** and **Move to quarantine** are available. If **Notify user in case of a threat** has been enabled, the user will also receive a notification.

Whenever Anti-Ransomware carries out an action, a report is added to the Security events tab. If a program has falsely been identified as a threat, the corresponding report can be used to create a

whitelist entry. Whitelist entries can be viewed and removed by clicking **Edit global whitelist**.

4.3.4.3. 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.
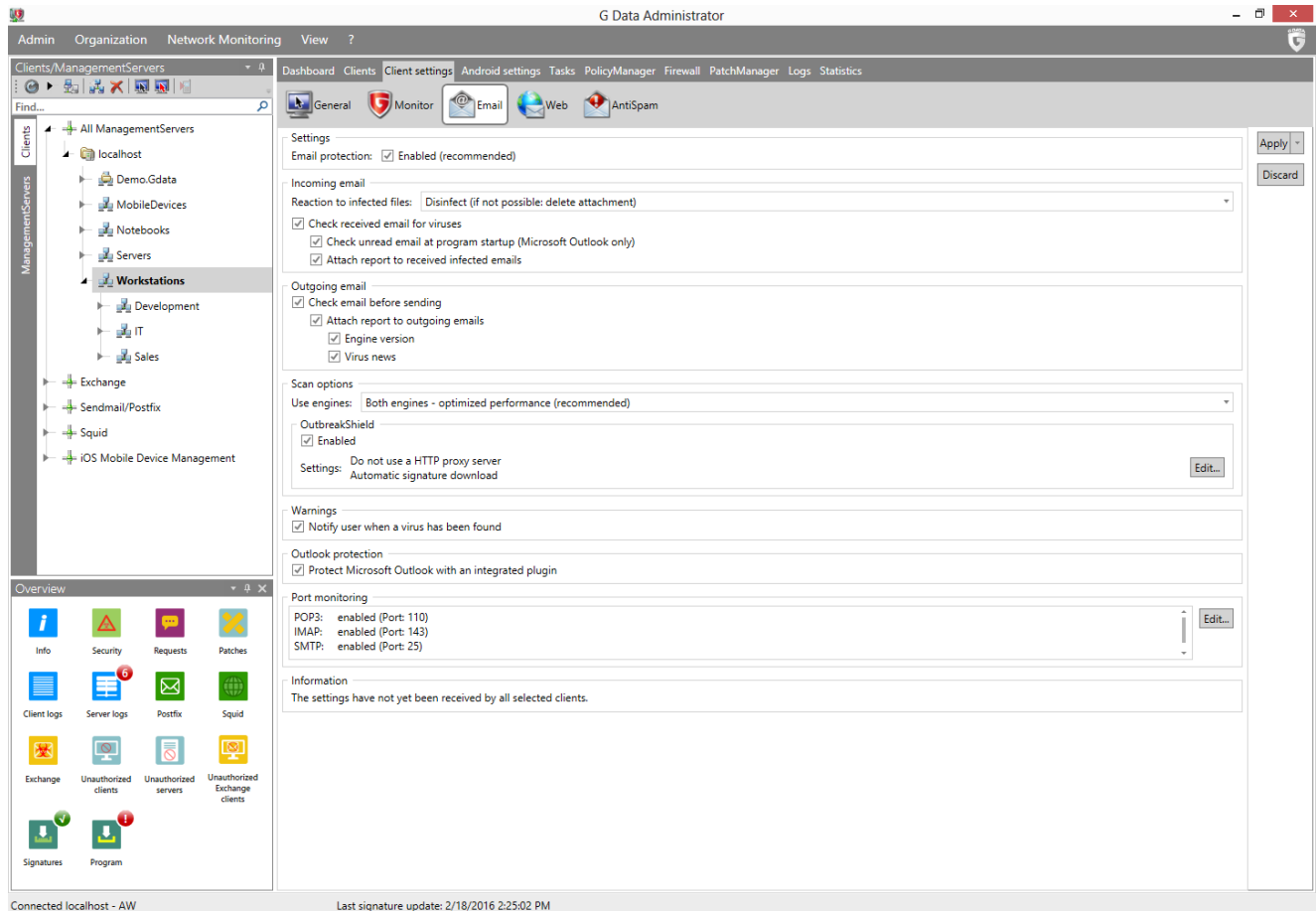
Incoming email

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 email beneath the actual email 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 displayed 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 can 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 pop-up.

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 **Scan 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.

4.3.4.4. Web

The Web panel allows you to define in-depth scan settings for internet traffic and online banking.

If you choose not to check Internet content, the **Monitor** will engage anyway when a user tries to access infected downloaded files. That means that the system on the respective client is also protected without checking Internet content, as long as the virus monitor is active.
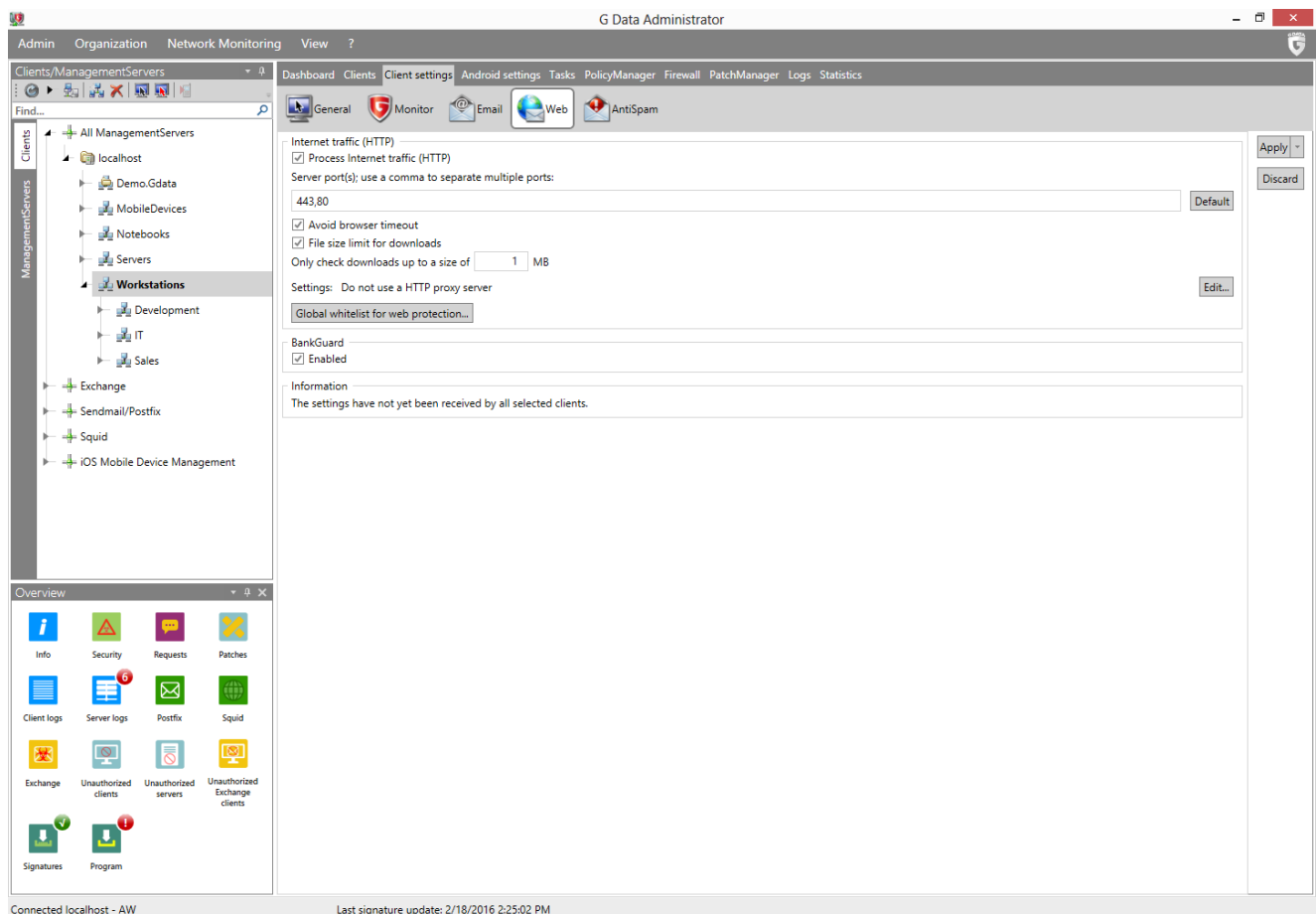
Internet traffic (HTTP)
The section Internet traffic (HTTP) covers scan settings for HTTP traffic.

- **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 Endpoint Protection Business) 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.

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.

4.3.4.5. AntiSpam

The AntiSpam module is available as part of the Client Security Business, Endpoint Protection Business and Managed Endpoint Security solutions.

If you check the option **Use spam filter**, client email traffic will be checked for possible spam mails. You can configure a warning message that will be added to the subject line when an email is identified as spam or falls under suspicion of being spam.
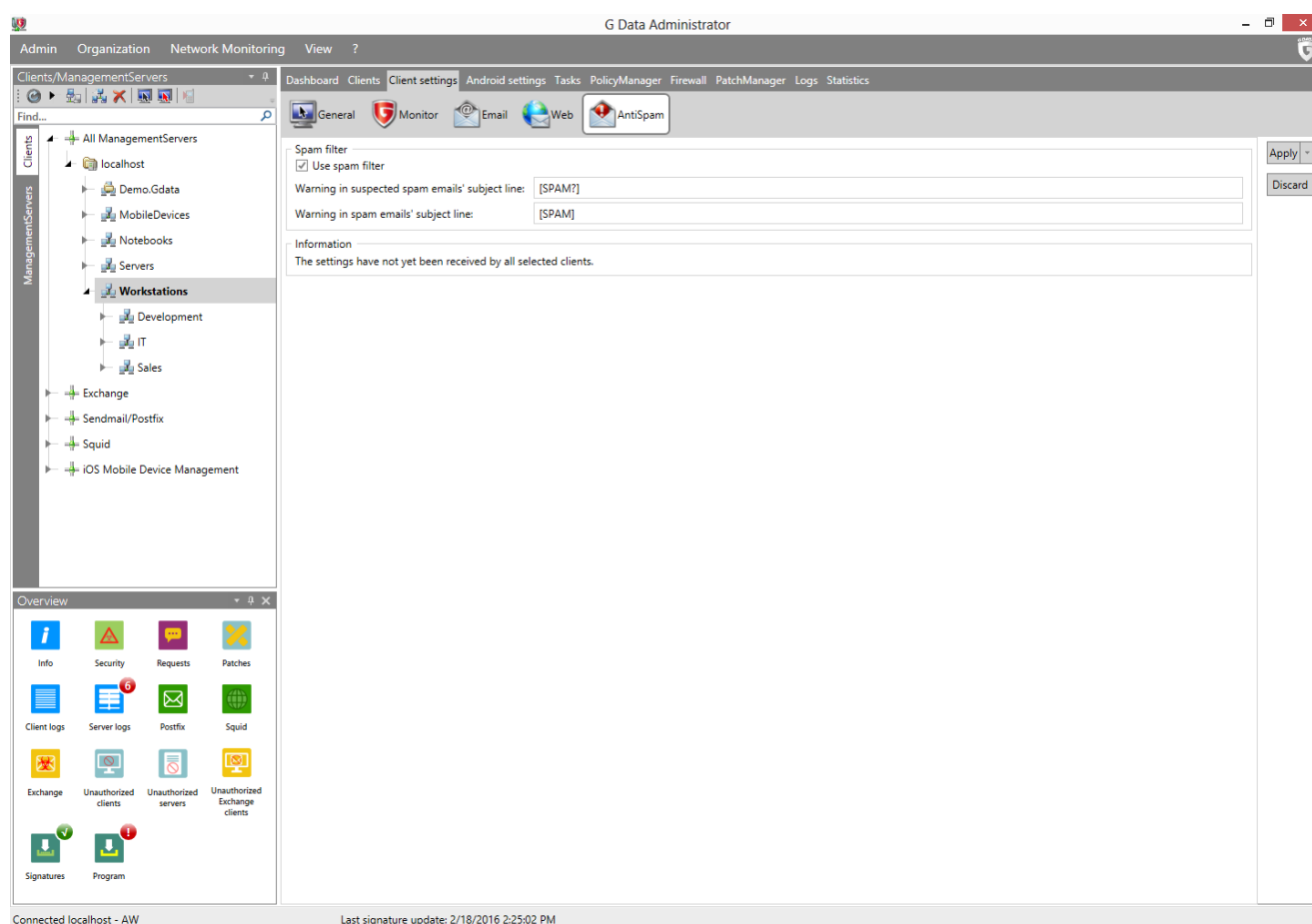
If the **Microsoft Outlook plugin** has been enabled, incoming spam mails will be moved to the AntiSpam folder. For other e-mail clients, spam mails can be automatically moved to a dedicated spam folder by defining a filter rule that matches the spam warning in the subject. To configure AntiSpam settings when using Microsoft Exchange, see **Exchange settings** > **AntiSpam**.

4.3.5. Exchange settings

G DATA Exchange Mail Security is available as an **optional module**.

The Exchange settings module offers access to settings for the Exchange plugin of G DATA MailSecurity. The module becomes available as soon as the plugin is installed on Exchange Server 2007 SP1, 2010 or 2013.

4.3.5.1. General

The General section lets you configure update settings, antivirus protection and scan settings for the Exchange plugin of MailSecurity.
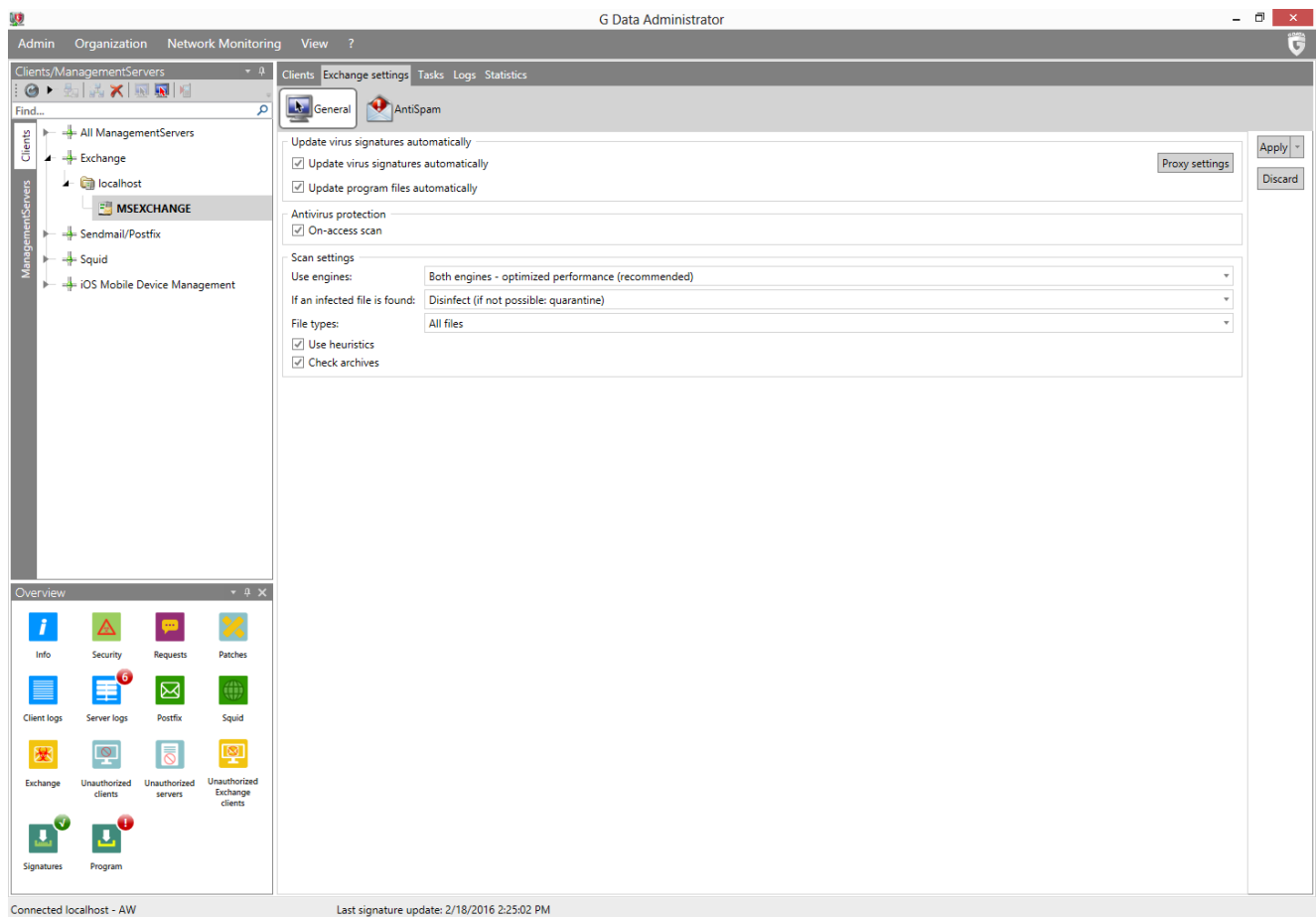
Update virus signatures automatically

Like regular clients, Exchange clients can be updated automatically.

- **Update virus signatures automatically**: Enables automatic updating of the virus signatures. At every **synchronization interval** the Exchange clients 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. At every **synchronization interval** the Exchange clients check whether updated program files exist on the G DATA ManagementServer. If updated program files are available, they are automatically installed on the client.

Antivirus protection

Enable antivirus protection by checking the **On-access scan** checkbox. The **On-access scan** checks all emails, attachments and other objects for malware as soon as they are received or sent. If any malicious content is found, the measures defined under **Scan settings** are carried out.

Scan settings

The scan settings are similar to those used for **Monitor** and **Scan jobs**.

- **Use engines**: Define whether both scan engines should be used or only one. The recommended setting is to use both scan engines.

- **If an infected file is found**: The Exchange plugin can take care of infected files in various ways

similar to the **Monitor**.

- **File types**: To speed up the scanning process, scans can be limited to program files and documents. However, it is recommended to check all files.

- **Use heuristics**: Heuristics enable detection of malware based on typical malware characteristics, as an addition to traditional signature-based recognition.

- **Check archives**: Archives can be checked for malware inside of them. If malware is found, the archive as a whole will be disinfected or removed, possibly including clean files. If you have configured quarantine measures, the complete email message (including the archive) will be quarantined.

4.3.5.2. AntiSpam

The AntiSpam option of the Exchange plugin makes sure that spam messages are filtered before they even reach the recipient. It is only available on Exchange servers that are running the Hub Transport role.

Spam messages are categorized in three distinct categories: **Suspected spam**, **High spam probability** and **Very high spam probability**. For each of those categories, you can customize the action that the Exchange plugin will take:

- **Reaction**
  - **Deliver email**: The email message will be delivered to the recipient.
  - **Move email to Quarantine**: The email message will be moved to the Quarantine folder.
  - **Reject email**: The email message will be rejected.
  - **Move email to Spam folder**: The email message will be moved to the Spam folder.
- **Subject prefix**: Add a prefix to the subject of the email message, such as a *[SPAM?]*tag.
- **Message in body**: Add text to the body of the email message.
- **Create reports**: Add a report to the **Security events** module.

In addition to the three spam categories, you can define a whitelist and a blacklist. Email messages from addresses or domains on the whitelist are never checked for spam; addresses and domains on the blacklist are always treated according to the configuration for **Very high spam probability**. The whitelist and blacklist can be exported and imported as .json files.
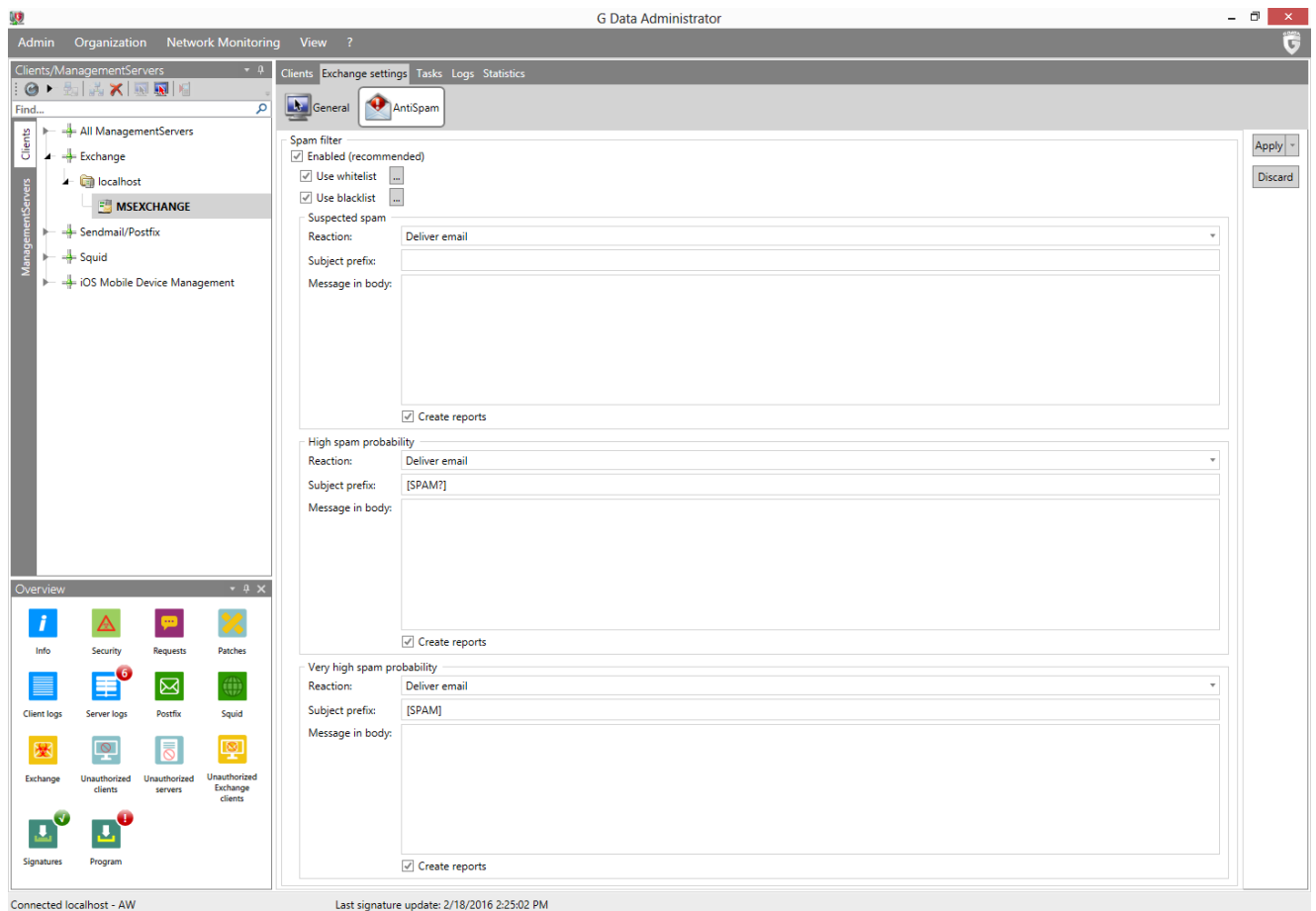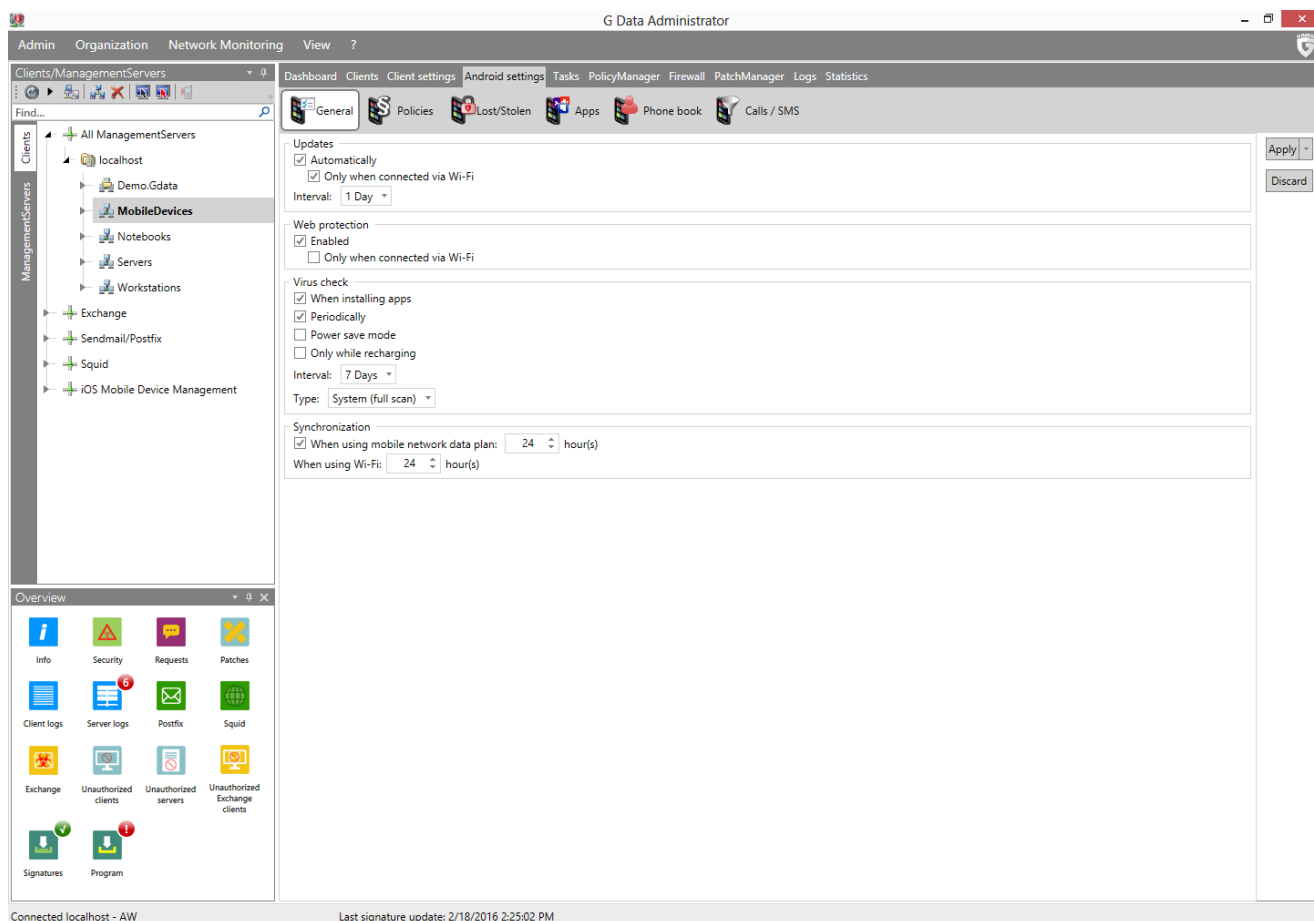
4.3.6. Android settings

The Android settings module offers easy access to G DATA Administrator's Android management capabilities.

4.3.6.1. General

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

- **Description**: 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 Android 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 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, web protection can be configured to only look up websites when there is Wi-Fi connectivity. The Web protection section therefore includes the possibility to limit web protection to wireless networks.

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

Virus check

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

- **When installing apps**: 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.
- **Only while recharging**: Run the periodic virus check only when the device is being charged.
- **Type**: Scan **System (full scan)** or only **Installed applications**.

Synchronization

The Synchronization option defines how often the Android 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.

4.3.6.2. 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.
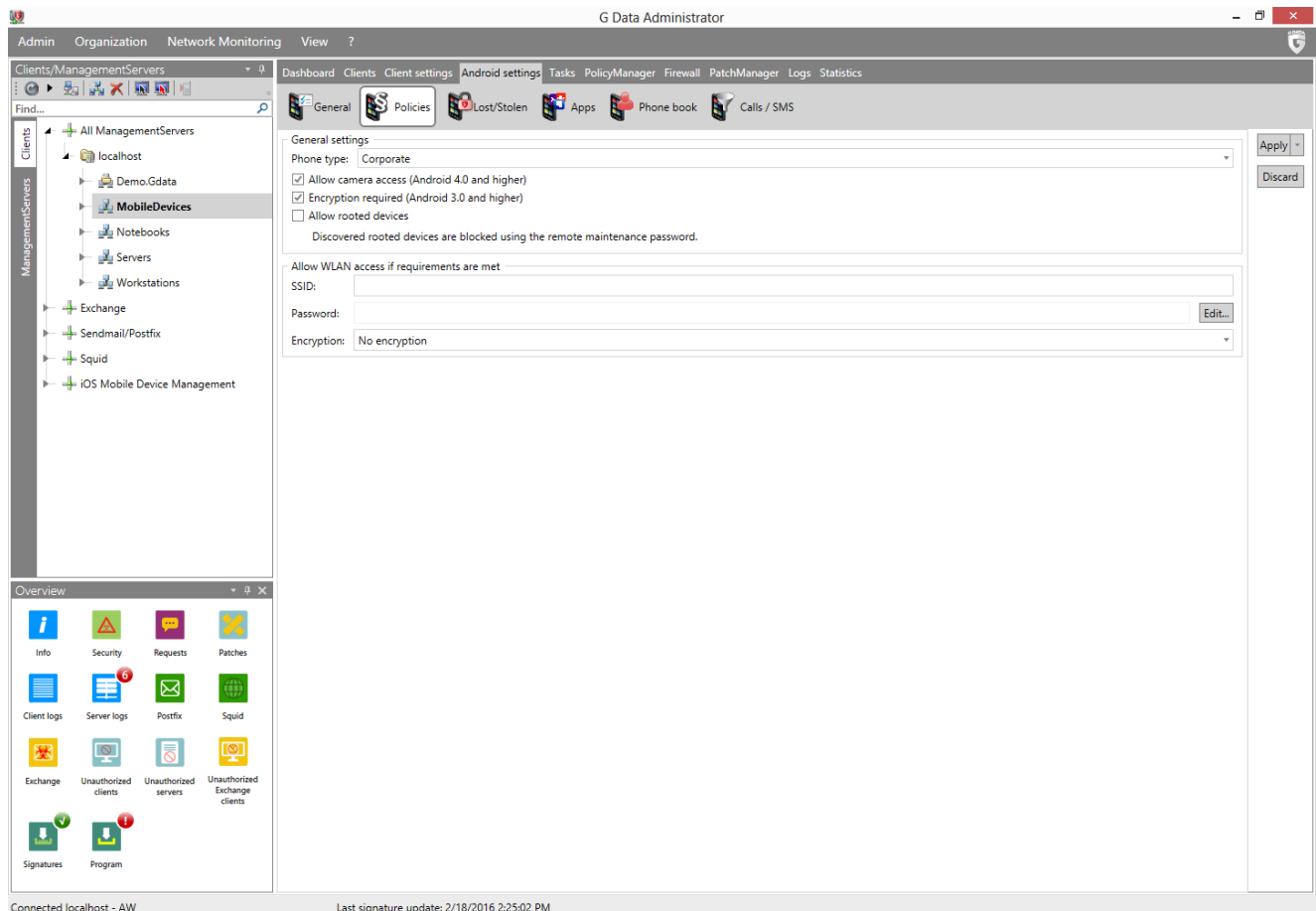
General settings

Under General settings, select the **Phone type** for the selected device(s). This decides which settings profile will be used by G DATA Internet Security for Android:

- **Corporate**: G DATA Internet Security for Android will use settings from the corporate profile, which is regularly synchronized with G DATA ManagementServer. The user is not allowed access to any settings. This is the recommended setting for corporate devices.

- **Private**: G DATA Internet Security for Android will use settings from the private profile, which is not synchronized with G DATA ManagementServer. The user is allowed access to all settings in G DATA Internet Security for Android.

- **Mixed**: The user can freely switch between the corporate and private profiles.

  Warning: When enabling **Private** or **Mixed** mode, the user will gain access to functionality that cannot be managed centrally. Using **Corporate** mode is recommended for all managed Android devices.

Regardless of the phone type, the following functions can be managed:

- **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 Lost/Stolen. If disabled, rooted devices cannot access the wireless network defined under Allow WLAN access if requirements are met.

Allow WLAN access if requirements are met

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

Enter the **SSID** for the corporate network for which access should be enabled. If the network is encrypted, enter the **Password** and select the **Encryption** type.

4.3.6.3. Lost/Stolen

The Lost/Stolen 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 Firebase Cloud Messaging, these anti-theft functions can also be triggered manually at any time.
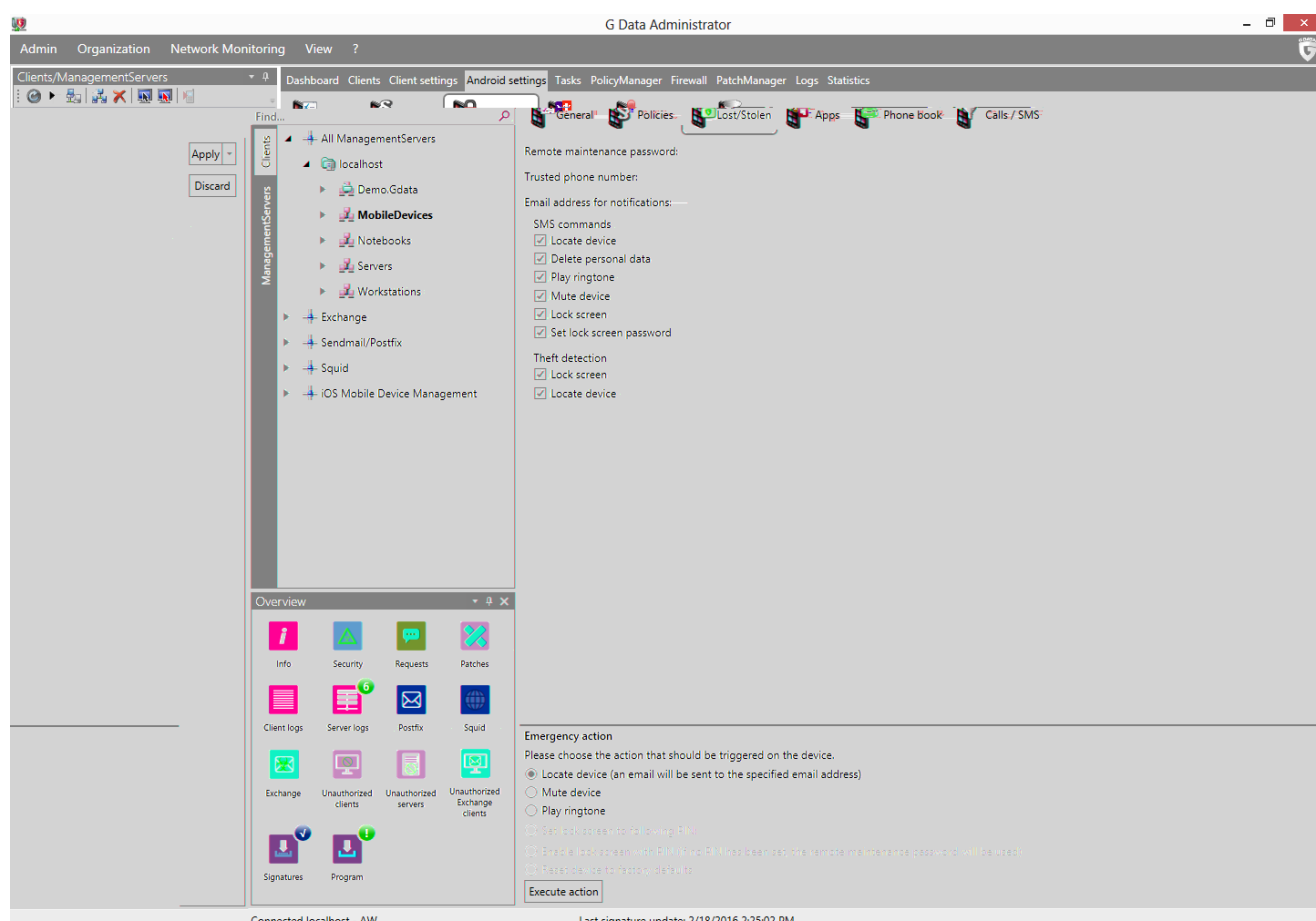
Before specifying any anti-theft measures, some general settings should be entered. The **Remote maintenance password** consists of numbers and functions as a PIN code. When sending SMS commands to the device, the password has to be included to ensure that only authorized users can send commands. The command to remotely reset the maintenance password can only be sent from the **Trusted phone number**. Some of the SMS commands trigger a report or other notification, which will be sent to the device from which the command was issued. Optionally, they can also be sent to an **Email address for notifications**. If you enable one or more of the Theft detection options, any

available location information will also be sent to this email address.

SMS commands

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

- **Locate device**: The device will report its location via SMS. If an email address has been entered under Lost/Stolen, location data will be sent there as well. To trigger this function, send an SMS containing the text *password***locate**.
- **Delete personal data**: The device will be reset to its factory settings. All personal data will be wiped. To trigger this function, send an SMS containing the text *password***wipe**.
- **Play ringtone**: The device will play a ringtone until Internet Security for Android is started. This will assist in locating lost devices. To trigger this function, send an SMS containing the text *password***ring**.
- **Mute device**: If you do not want the device to call attention to itself with ring tones or other signals, it can be muted. This does not include the ring tone that is used to locate lost devices. To trigger this function, send an SMS containing the text *password***mute**.
- **Lock screen**: The device screen can be locked to prevent the device from being used. To trigger this function, 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 after sending the lock command. To trigger this function, 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*.

Theft detection

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.

- **Lock screen**: same functionality as the option under SMS commands.
- **Locate device**: same functionality as the option under SMS commands.

Emergency action

Using the internet-based Firebase Cloud Messaging framework, emergency actions can be triggered on Android devices. This has the advantage of working even if a device is being used without a SIM card. Firebase Cloud Messaging must be configured under **General settings** > Android before using any emergency actions.

Select any of the following actions and click **Execute action** to send the command to the device:

- **Locate device**: same functionality as the option under SMS commands.
- **Mute device**: same functionality as the option under SMS commands.
- **Play ringtone**: same functionality as the option under SMS commands.

- **Set lock screen to following PIN**: same functionality as the option under **SMS commands**.
- **Enable lock screen with PIN**: same functionality as the option under **SMS commands**.
- **Reset device to factory defaults**: same functionality as the option under **SMS commands**.

4.3.6.4. 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** and **Size**. 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**.

4.3.6.5. 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.
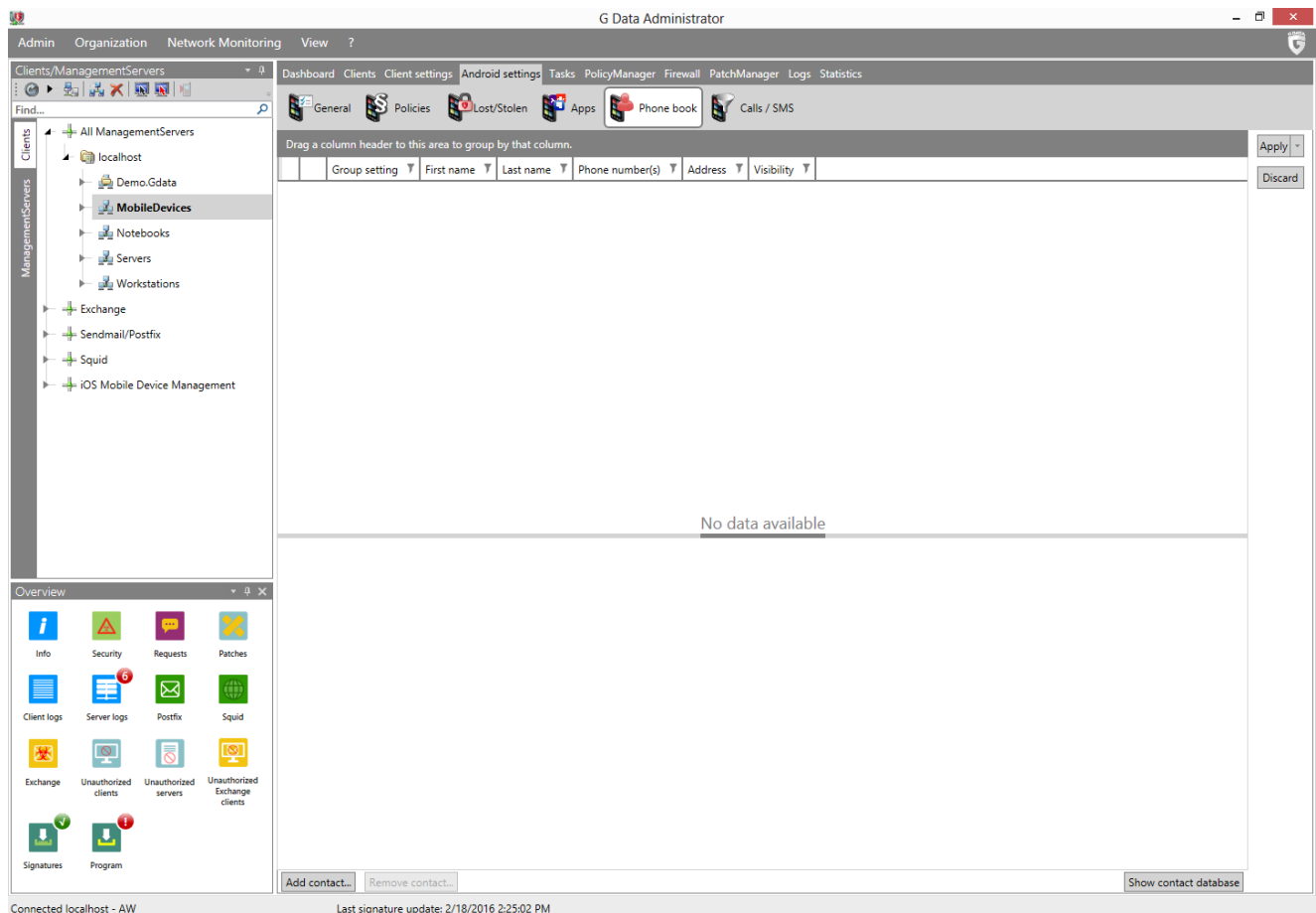
The main list shows all contacts that have been added to Internet Security's phone book. For each contact, the **First name**, **Last name**, **Phone number**(s) and **Address** are listed. Using the **Visibility** dropdown menu, you can decide whether the contact should be **Visible** in the Android 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 email 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.

4.3.6.6. Calls / SMS

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.
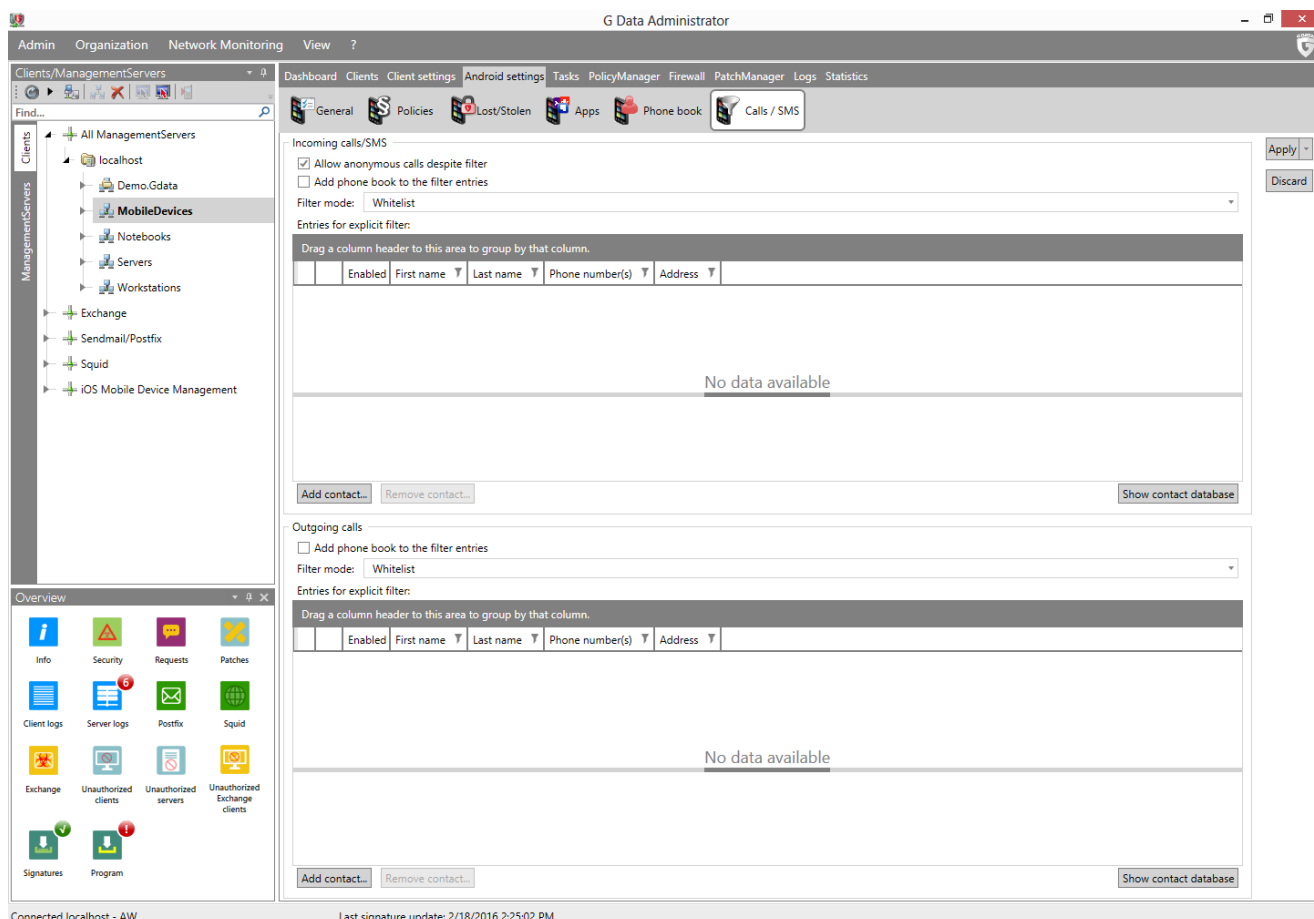
Incoming calls/SMS

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. Enabling the additional option **Add phone book to the filter entries** will allow contacts with an entry in the Android or Internet Security phone books through the filter, in addition to any whitelisted contacts.

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. Enabling the additional option **Add phone book to the filter entries** will allow contacts with an entry in the Android or Internet Security phone books to be contacted, in addition to any whitelisted contacts.

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 permitted. The permission request will be added to the **Security events** module. It can be used by the administrator to directly add a blacklist or whitelist exception for the

contact.

4.3.7. iOS settings

The iOS settings module offers easy access to G DATA Administrator's iOS management capabilities.

4.3.7.1. General

Using the General tab, you can enter a note for the selected client(s) and assign a profile:

- **Description**: Enter a note, for example information about the device or its configuration. The note is only displayed in G DATA Administrator.

- **Active profile**: Displays the currently assigned profile. Select a profile from the list to change the profile or select **- No profile -** to remove the current profile.

In addition to the note and profile settings, the General tab also displays settings that have been configured when Device Management was deployed to the device. This includes the Device Management name, description, organization and the End User License Agreement.
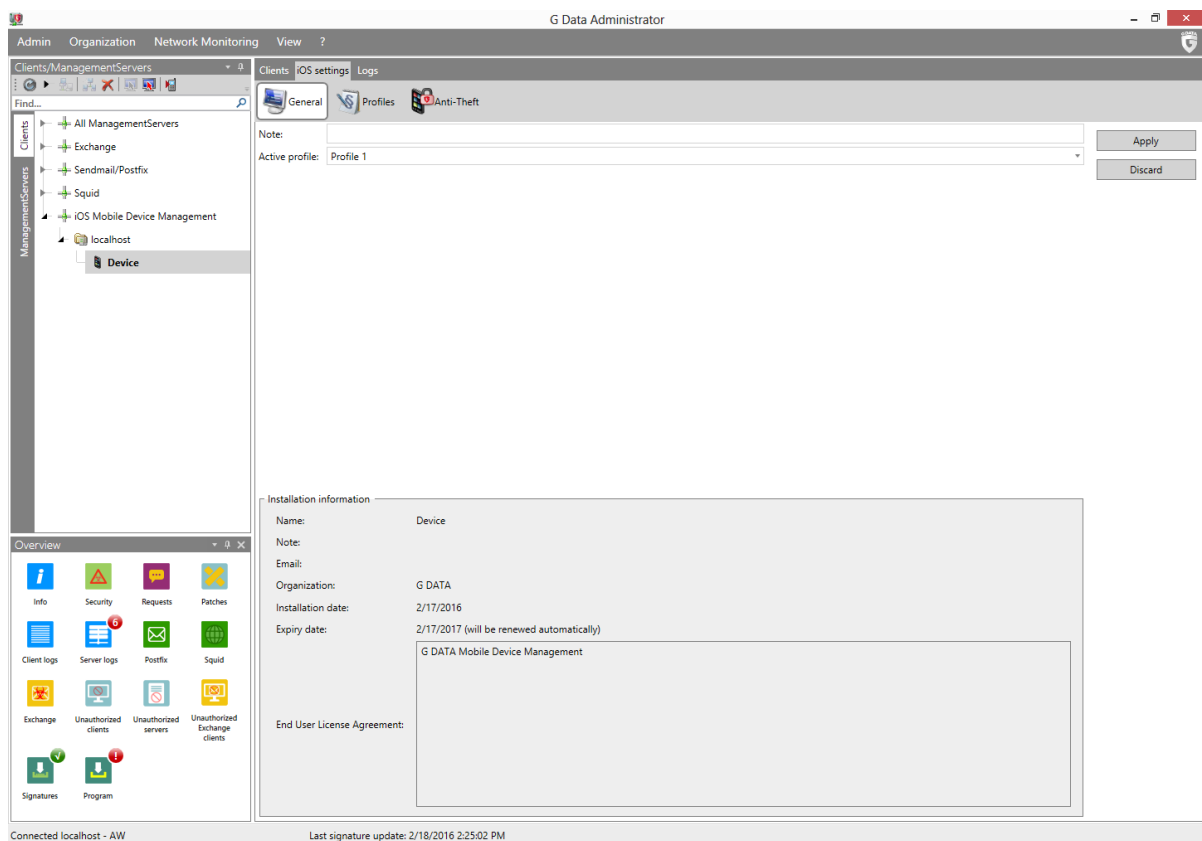
4.3.7.2. Profiles

Using profiles you can deploy security policies to (groups of) iOS devices. Use the Add profile toolbar button to define a new profile by entering its **Name** and a **Description** (optional). Each profile can contain up to five policies, each focusing on a specific branch of settings. Under **Add policy**, select one of the following five policies and click the plus sign to add it to the profile:

- **Functionality restrictions**: Disable specific functions of the iOS device (such as camera usage, Siri or iCloud).

- **App restrictions**: Disable specific apps or app settings (such as YouTube, iTunes Store or Safari).

- **Media content restrictions**: Disable specific types of media content, based on various rating

systems.

- **Passcode settings**: Enforce iOS passcode standards (such as minimum length, minimum complexity and a maximum number of failed attempts).

- **WLAN**: Allow the iOS device to connect to a specific wireless network.

Select a policy to edit its settings. Click **Apply** to save the profile and all its policies. If you are editing a profile that has already been assigned to a device, the updated profile will be synchronized with the device and a report will be added to the **Logs (iOS)** module as soon as the device has applied it.
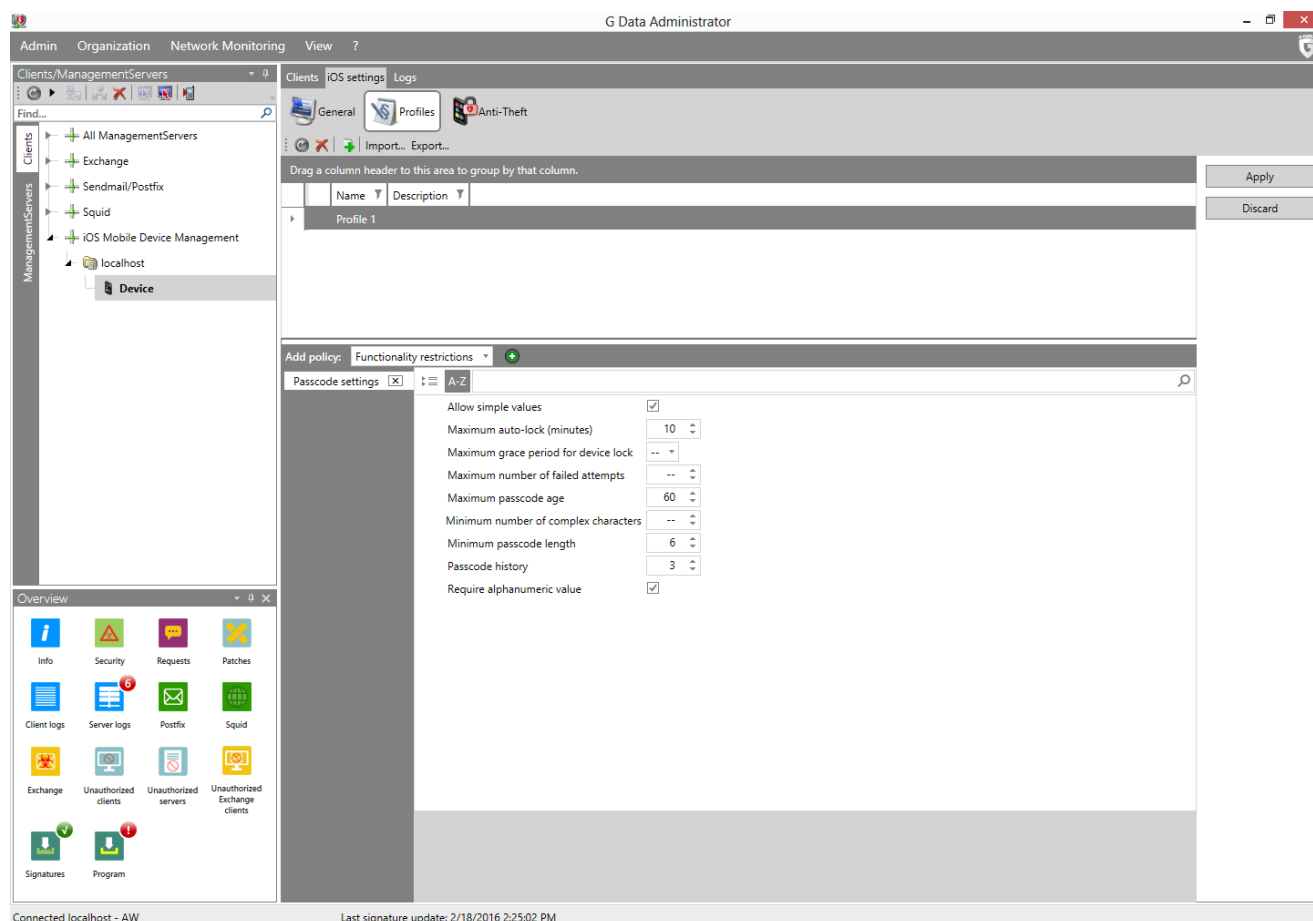
Profiles can be imported and exported by clicking the respective buttons. Profile settings are saved as a JSON file.

4.3.7.3. Anti-Theft

The Anti-Theft tab lets you trigger one of three anti-theft actions on the selected iOS device:

- **Lock device**: The device's lock screen will be enabled (including passcode protection, if a passcode has been set).

- **Reset device**: The device will be wiped. Warning: this removes all data and also disables Device Management.

- **Remove passcode**: The device's passcode will be removed.

Click **Execute function** to carry out the selected action. The status will be reported under **Logs (iOS)**.
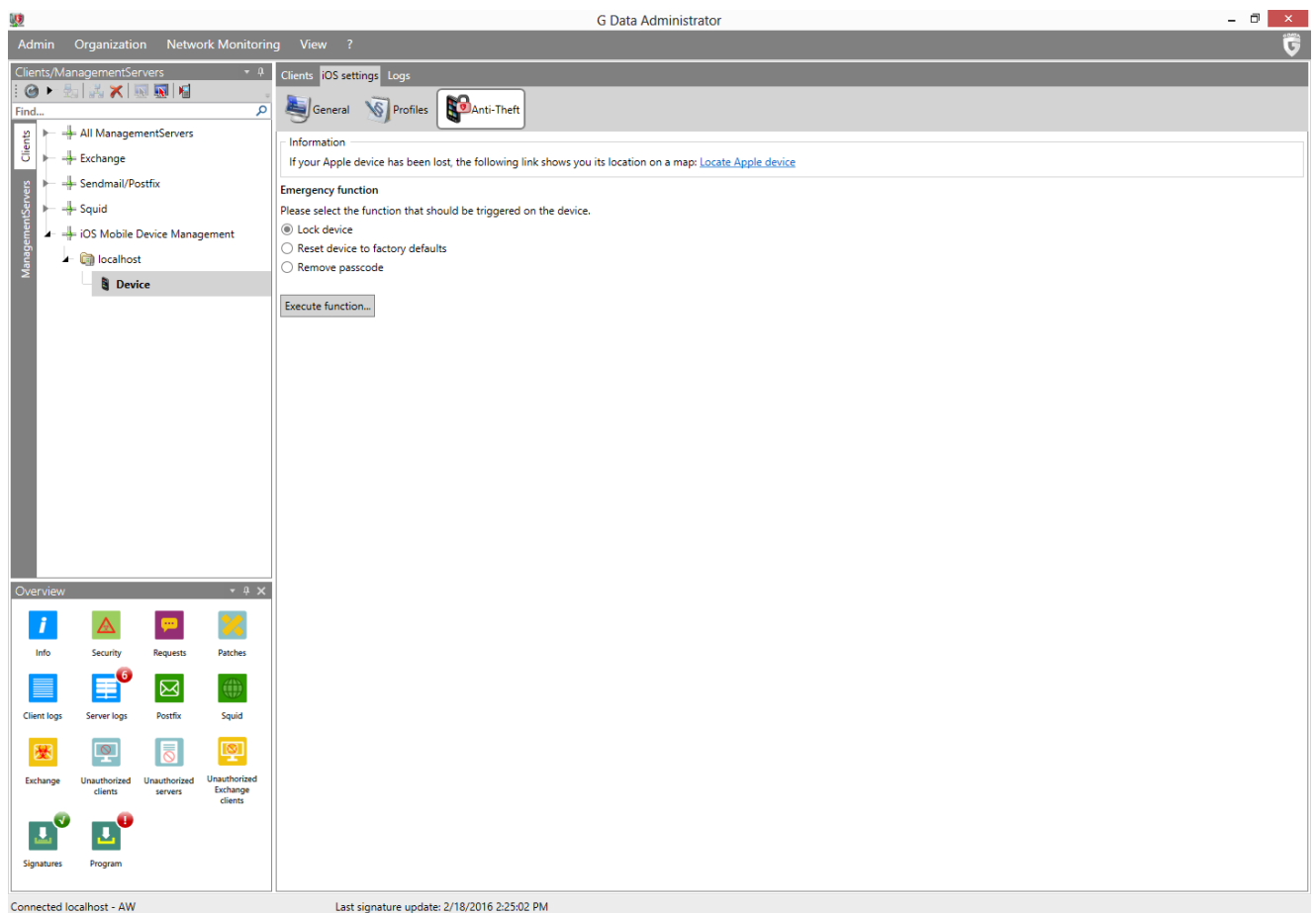
4.3.8. Sendmail/Postfix

The Linux Mail Security Gateway module is available as an **optional module**.

The **Sendmail/Postfix** module offers access to settings for Linux Mail Security Gateway.

4.3.8.1. Settings

Under Settings, the antivirus protection can be configured:

- **Reaction**: Define the reaction to infected emails (**Delete infected attachments** or **Move email to quarantine**).
- **Subject prefix**: Add a prefix to the email subject (e.g. *[VIRUS]*).
- **Message in body**: Add a notification to the email body (e.g. *This email contains a virus*).
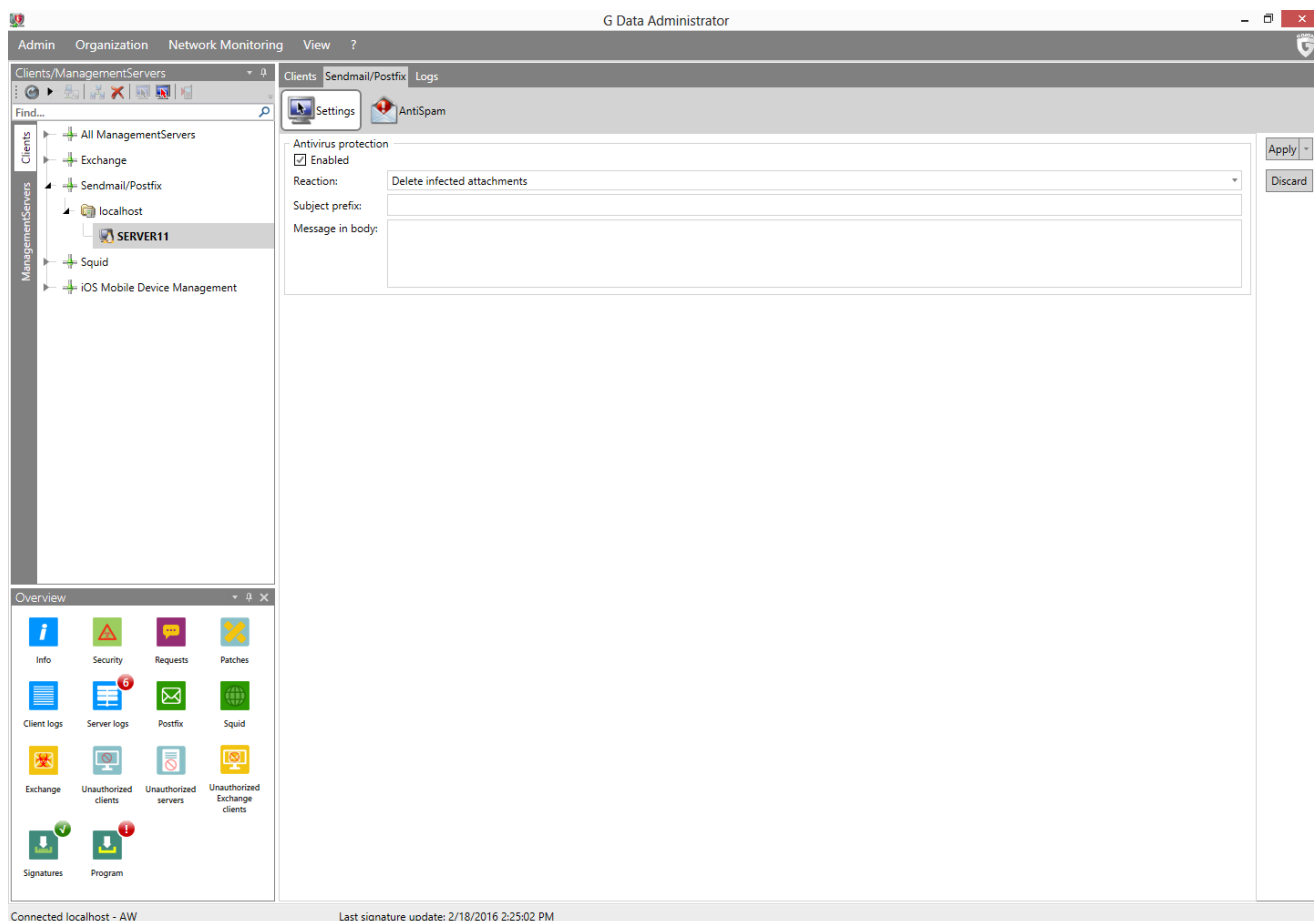
4.3.8.2. AntiSpam

Using the AntiSpam settings, the Linux Mail Security Gateway module automatically filters incoming email for spam.
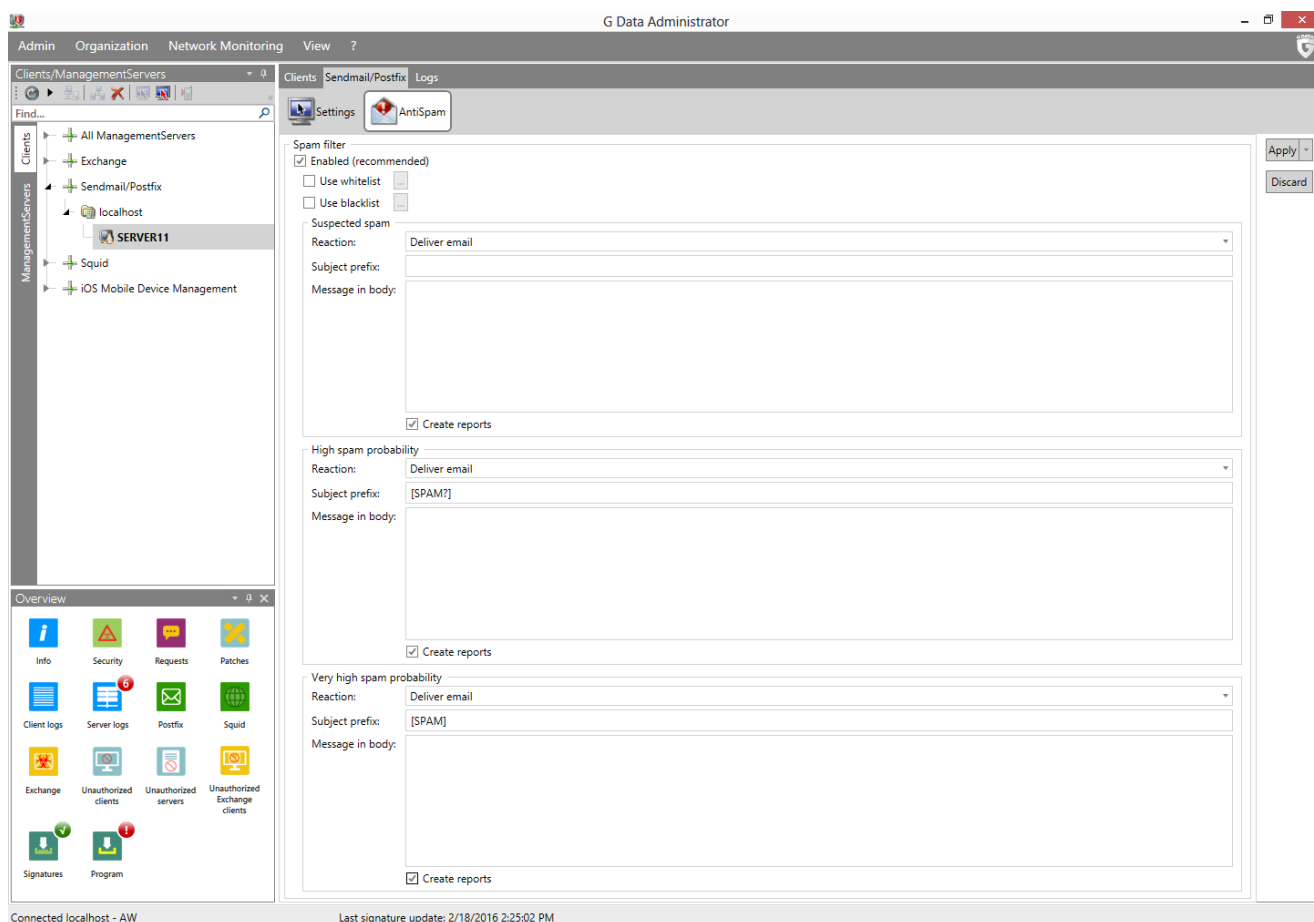
Spam messages are categorized in three distinct categories: **Suspected spam**, **High spam probability** and **Very high spam probability**. For each of those categories, you can customize the action that the plugin will take:

- **Reaction**
  - **Deliver email**: The email message will be delivered to the recipient.
  - **Delete message**: The email message will be deleted.
- **Subject prefix**: Add a prefix to the subject of the email message, such as a *[SPAM?]*tag.
- **Message in body**: Add text to the body of the email message.
- **Create reports**: Add a report to the Security events module.

In addition to the three spam categories, you can define a whitelist and a blacklist. Email messages from addresses or domains on the whitelist are never checked for spam; addresses and domains on the blacklist are always treated according to the configuration for **Very high spam probability**. The whitelist and blacklist can be exported and imported as .json files.

4.3.9. Squid

The Linux Web Security Gateway module is available as an optional module.
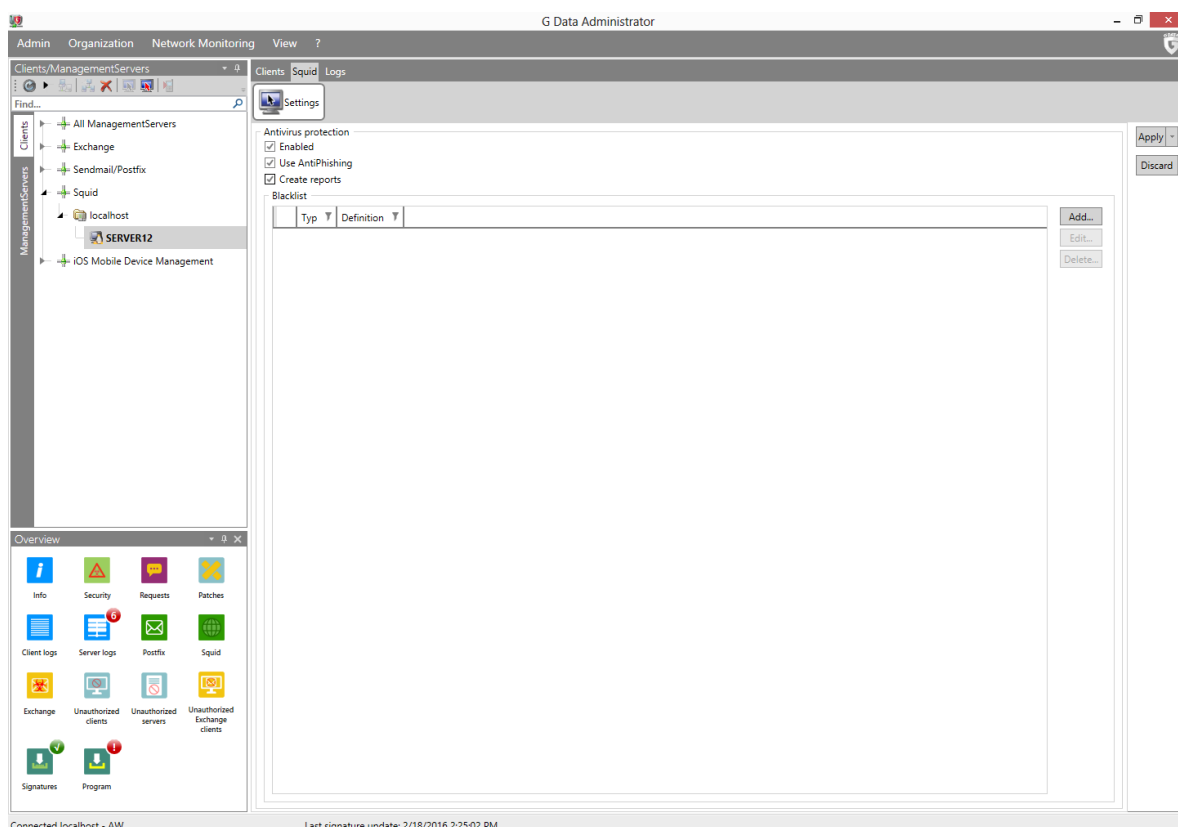
The **Squid** module can be used to configure settings for the Linux Web Security Gateway. Under **Antivirus protection**, the following settings can be configured:

- **Enabled**: Enable the antivirus protection for Squid.
- **Use AntiPhishing**: Enable cloud lookups to enhance protection.
- **Create reports**: Add a report to the Security events module when a virus is found.

Under **Blacklist**, click **Add** to add a **Domain**, **Proxy client IP address** or **MIME type** to the blacklist. Entries on the blacklist are always blocked.

4.3.10. Tasks

In the Tasks module you can define client and group tasks (jobs). There are two different job types: single jobs and periodic jobs. Single jobs are performed once at a specific time; for 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 time.
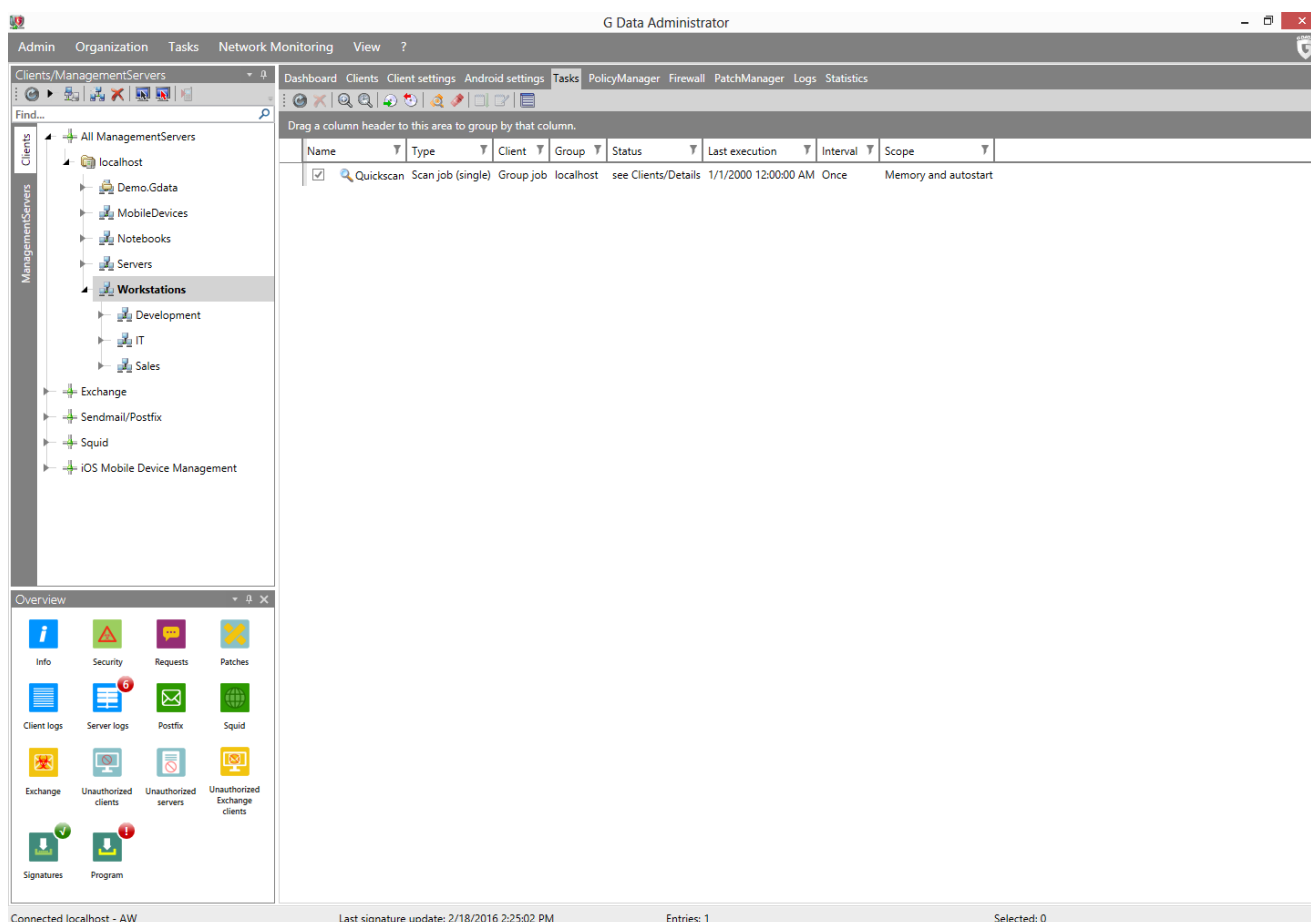
In the Tasks area, the following data are listed for every job:

- **Name**: The job name you entered. You can enter a name of any length.
- **Type**: The type of job, such as a scan job or a software recognition job.
- **Client**: The clients for which the job was created. You can only create jobs for enabled clients.
- **Group**: If you create a group job, the group name will be displayed, rather than the individual clients.
- **Status**: The status or the results of a job. For example, you can see whether the job has just run or has been completed, and also find out if 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) are included in the job.

To edit tasks, select the **Properties** command from the context menu (by right-clicking).

The following options are available in the toolbar above the task list:

- **Refresh**
- **Delete**

🔍 **Single scan job**: Define a single scan job for clients or client groups. In the configuration dialog, the time, scope, and additional scan settings can be defined on their respective tabs.

🔍 **Periodic scan job**: Define a periodic scan job.

🔄 **Backup job**: Define a backup job for clients or client groups (optional Backup **module**).

🕐 **Restore job**: This function allows you to restore backups to clients or groups (optional Backup **module**).

🔍 **Patch applicability job**: List software and patches that have been installed on clients (optional PatchManager **module**).

✏ **Software distribution job**: Schedule software and patch distribution (optional PatchManager **module**).

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

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

📄 **Display 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:

- **Display group jobs in detail**

- **Run now**: Re-run single scan jobs which have already been run or canceled. 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 (optional Backup **module**).

- **Add**: Create a job.

4.3.10.1. Scan jobs

The **New 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.

Which options are available on the tabs depends on the type of client that the job is being planned for. For example, when planning a job for an Exchange server (if Exchange Mail Security has been installed), options that deal with threats specific to desktop clients are not available.

Job scheduling
The **Job scheduling** tab lets you plan the scan job:

- **Job name**: 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.

- **Schedule** (Periodic scan job): For periodic scan jobs, this option 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.

- **Time**: Use this option to set a specific start time. For single scan jobs without start time, the scan job will be started immediately after creation.
- **Settings**
  - **Allow the user to halt or cancel the scan job**: Permissions can be granted to the users for pausing or aborting the job via the system tray context menu.
  - **Notify the user when a virus has been found**: Displays a notification on the client when a virus is found.
  - **Report scan progress to the ManagementServer (every 2 minutes)**: Enable this option to report the status of a scan job to the server.
  - **Shut down client after scan job, if no user is logged on**: The client can be shut down automatically after the scan job is finished.
  - **Run scan job later if a client is not powered up at the scheduled time**: 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 this option.
- **User context (optional)**: If the scan job includes network shares, they should be entered as a UNC path instead of using mapped network drives. If the client's machine account (e.g. *Client001$*) has no permissions to access a share, enter a **User name** and **Password** for an account with the appropriate permissions here.


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 (see **Client settings** > **Monitor**).
- **If an infected file is found**: Specify what should happen if an infected file is detected (see **Client settings** > **Monitor**).
- **Infected archives**: Specify here how infected archives are to be treated (see **Client settings** > **Monitor**).
- **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).
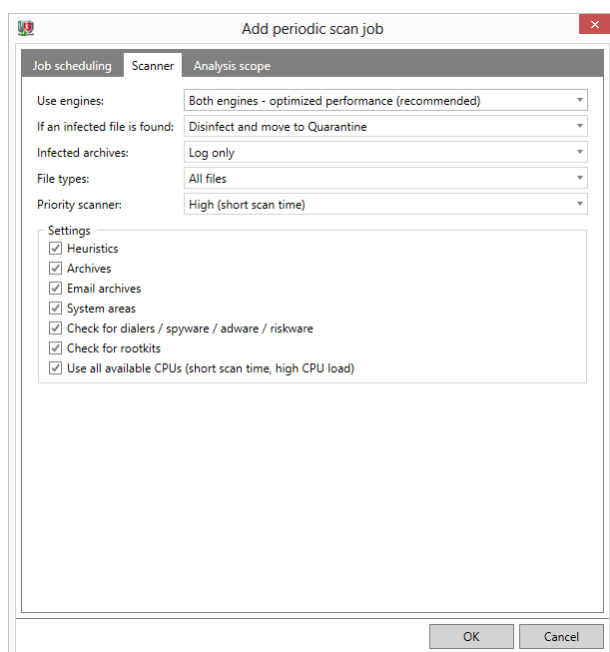
Analysis scope

Using the Analysis scope tab, you can limit the scan job to specific directories (when planning a scan job for a client) or mailboxes (when planning a scan job for an Exchange server). The folder selection window allows you to pick folders from both the PC on which Administrator is running and on clients. When including network shares, they should be defined as a UNC path instead of using mapped drives. The Analysis scope can be used to exclude folders, for example those with rarely used archives (which can then be checked in a separate scan job).
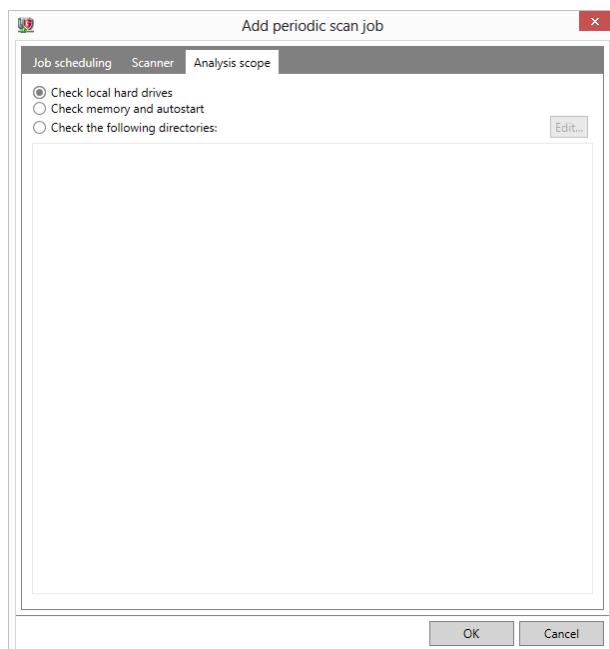
4.3.10.2. Backup jobs

Backup is available as an **optional module**.

Using backup jobs, administrators can plan backup tasks for client data in order to centrally safeguard essential files.

Job scheduling
A **Job name** for the backup job must 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 needs to be rebuilt from multiple backup files.
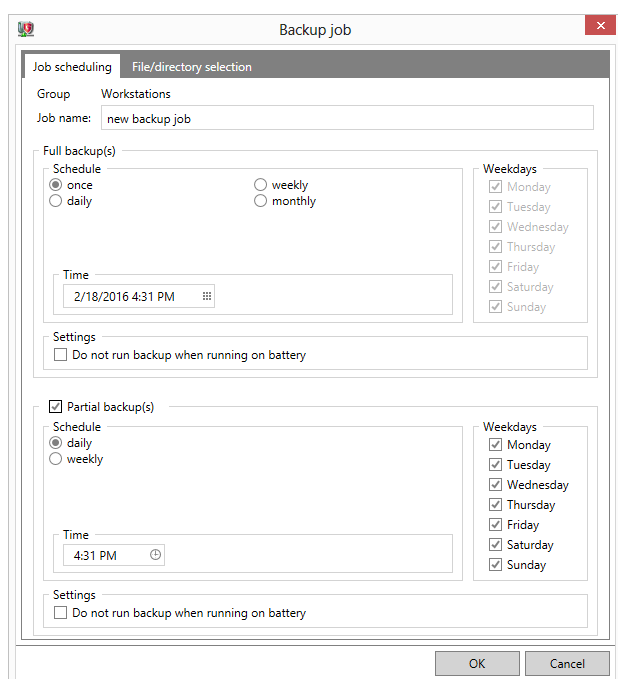
Enable **Do not run backup when running on battery** to prevent burdening mobile computers running in battery mode with a backup job. The backup will be postponed until the client is connected to a power supply. For **Daily** jobs, you can specify under **Weekdays** on which specific days of the week

the job should be carried out.

Server-side backup storage paths as well as quota notifications can be configured under **General settings** > **Backup**.

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, G DATA Security Client will always buffer the backup on the partition containing the most free disk space. The directory G DATA\Backup will be created in the root directory of the partition.
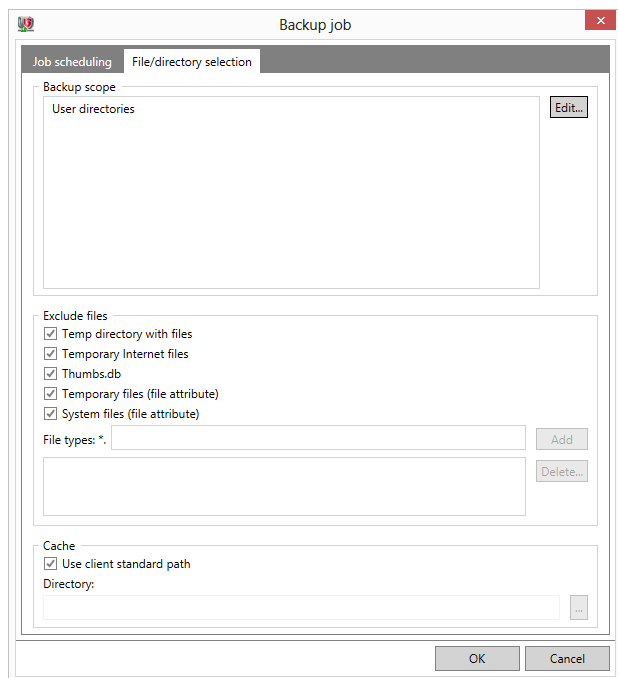
4.3.10.3. Restore jobs

Backup is available as an **optional module**.

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. For every 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 from which the files were backed up). 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.

4.3.10.4. Patch applicability jobs

PatchManager is available as an **optional module**.

Patch applicability jobs can be planned to check if one or more patches are applicable to clients or groups.

Patch applicability jobs can be scheduled using the following options:

- **Execution**: Decide when the patch applicability job should be run:
  - **Scheduled**: Run the patch applicability job according to a **Schedule**, which can be defined using one of the following parameters: **Immediately**, **Once**, **Hourly**, **Daily**, **Weekly**, **Monthly** or **On Internet connection**.
  - **As soon as available**: Run the patch applicability job each time a new patch is released.

To select the patches for which applicability should be checked, use one of the two **Scope** options:

- **Specific patch**: Choose one or more patches from a list.
- **Using attributes**: Use **Attributes** to select a range of patches using keywords. To add a specific attribute (**Vendor**, **Product name**, **Urgency**, **Language**) as a filter criterium, tick the checkbox and enter a keyword. This way you can check applicability for patches from a specific publisher or only for specific versions. Wildcards like `?`and `*`can be used. Enable the option

Patches only if the job should not check full software packages and upgrades for applicability.

Select **Automatically install applicable patches** to make sure that each time a patch is found to be applicable, it is installed automatically.

If the Patch applicability job is being planned from PatchManager's **Status overview** module, the job applies to the patch and clients that were selected there. If it is being planned from the **Patch configuration** module, you need to select the client(s) for which applicability should be checked. If it is being planned from the **Tasks** module, you need to select the patch(es) for which applicability should be checked - the job will be run on the currently selected group or client.

4.3.10.5. Software distribution jobs

PatchManager is available as an **optional module**.

To distribute **applicable patches** to clients or groups, you can define a software distribution job.

Software distribution jobs can be managed and scheduled using the **Planning** options:

- **Immediately**: The software distribution job will be run immediately.
- **Immediately after the boot process**: The software distribution job will be run after the next boot.
- **Immediately after logging in**: The software distribution job will be run after the next time an end user logs in to the client.
- **Only load at specified time**: Schedule the job to be run at a specific time (the other scheduling options will not come into effect until this point in time has been reached).
- **Load with delay**: Schedule a delay in starting the job. That way, the boot process and distribution job won't influence client performance at the same time.

If the Software distribution job is being planned from PatchManager's **Status overview** module, the job applies to the patch and clients that were selected there. If it is being planned from the **Patch configuration** module, you need to select the client(s) on which the patch should be installed. If it is

being planned from the Tasks module, you need to select the patch(es) that need to be installed - they will be installed on the currently selected group or client.

4.3.10.6. Rollback jobs

PatchManager is available as an optional module.

Using rollback jobs you can uninstall previously deployed patches. Right-click the respective distribution job in the Tasks overview and choose Rollback. Alternatively, select the specific client and patch in PatchManager's Status overview panel and choose Rollback from the context menu.

The Update rollback window lets you enter a Job name to easily identify the rollback job. After entering the name, click OK to add the job to the Tasks list. It will be executed immediately.

4.3.11. PolicyManager

The PolicyManager module is available as part of the Endpoint Protection Business and Managed Endpoint Security 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 and which programs may be used on the company PCs.

4.3.11.1. Application control

Application control can be used to restrict the use of specific programs. Under Status, specify whether the limitations should apply to all users (including administrators) or only to users who do not have administrator rights on the client.

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 **...** 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).

4.3.11.2. 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**, specify whether the limitations should apply to all users (including administrators) or only to users who do not have administrator rights on the client.

Under **Devices**, device usage can be restricted per **Device** type using the following settings:

- **Permission**
  - **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.
- **Temporary permission**: If a device has been temporarily permitted through a PolicyManager request in the Security events module, the time frame is displayed here. Click the X icon to cancel the temporary permission.

By using the **Exceptions** settings, you can allow access to devices to which you had previously limited access in some way or another (**Read** / **Deny access**). When you click the **Add** button a dialog window opens in which you can define a new exception:

- **Device**: Select the type of device for which you are adding an exception.
- **Rule enabled**: The exception is only active if this checkbox is selected.
- **Type**
  - **Device type exception**: The exception will be defined for the selected **Device** type as a whole.
  - **Hardware ID/medium ID exception**: The exception will be defined for a specific instance of the selected **Device** type (e.g. a specific DVD or USB stick), to be specified under **Hardware ID/medium ID**.
- **Permission**: Select the type of permission to be allowed.
- **Hardware ID/medium ID**: If you have selected **Hardware ID/medium ID exception**, enter the respective ID here. Click the **...** button to determine a specific hardware or medium ID:
  - **Select source**: Select **(Local search...)** to look for hardware and media IDs on computer on which G DATA Administrator is installed. Alternatively, select a client from the list to look for IDs on the respective client computer.
  - **Device**: Select **Use medium ID** to display IDs of media (e.g. CD/DVD) or **Use hardware ID** to display IDs of hardware.
- **Configure Windows users/groups**: If the exception should be limited to specific Windows users of groups, enter them here. Multiple entries should be separated by commas or line breaks.
- **Note**: Add a note to the exception (e.g. to be able to tell similar exceptions apart).

4.3.11.3. 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**, specify whether the limitations should apply to all users (including administrators) or
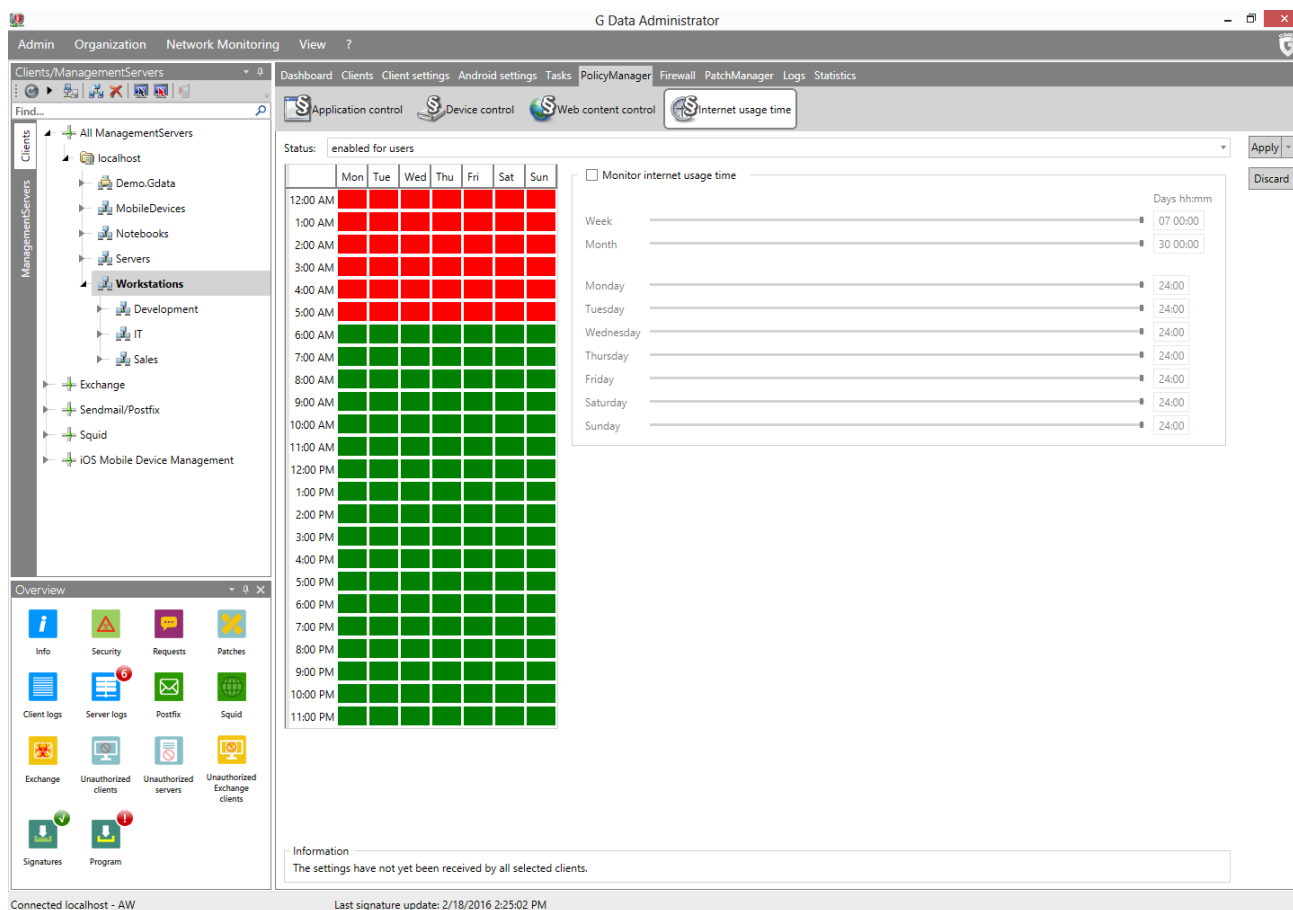
only to users who do not have administrator rights on the client.

Under **Global exceptions**, it is possible to ensure that certain websites are blocked or allowed company-wide across the entire network, regardless of any settings that have been made under **Allowed categories**. To do this, click **Add**, select **Allow** or **Block**, enter the **Address** (without protocol) and click **OK** to add the exception. Click **Edit** to edit an existing exception or **Delete** to delete exception(s).
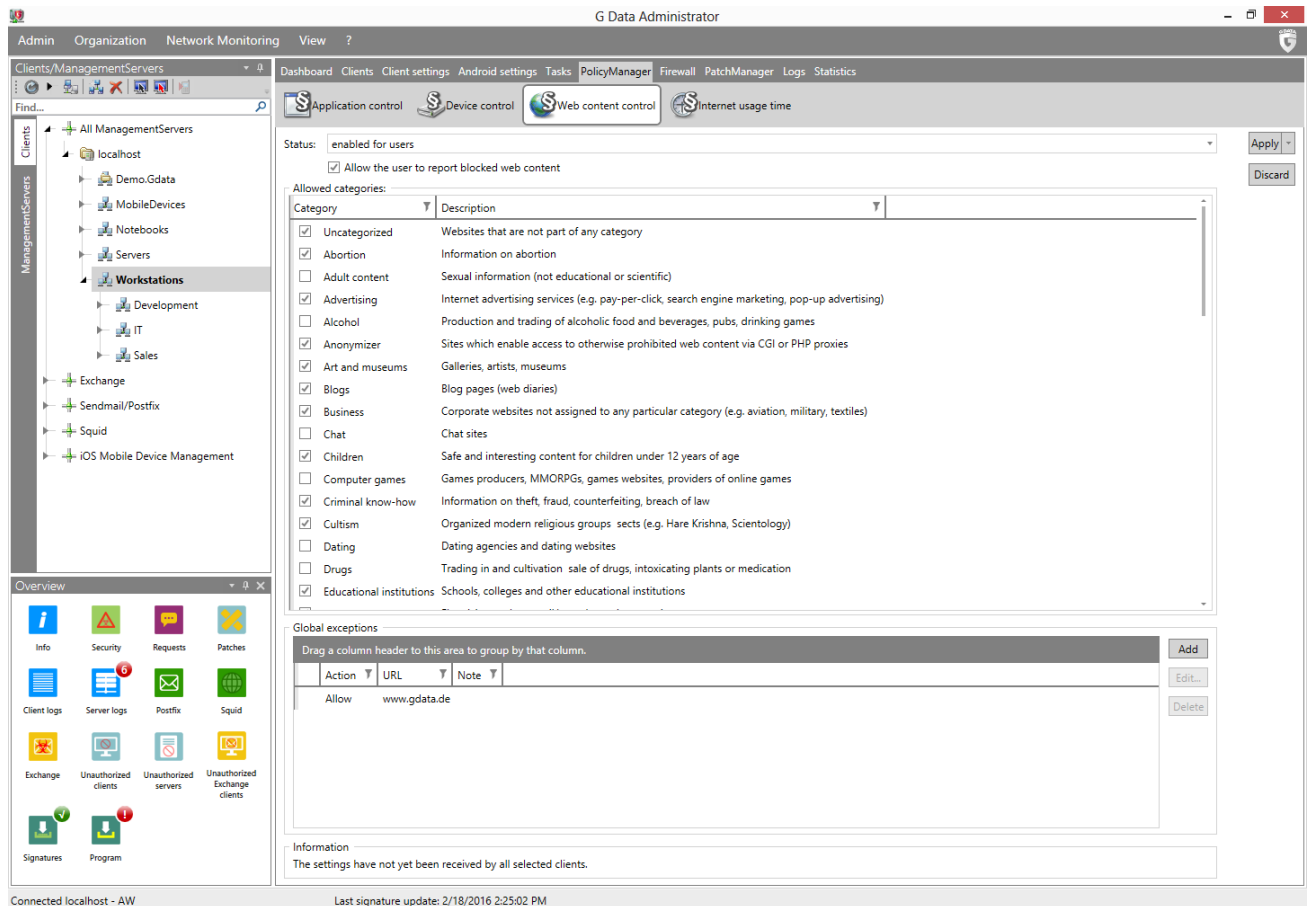
4.3.11.4. Internet usage time

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**, specify whether the limitations should apply to all users (including administrators) or only to users who do not have administrator rights on the client. 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 area with time restrictions 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.

4.3.12. Firewall

The Firewall module is available as part of the Client Security Business, Endpoint Protection Business and Managed Endpoint Security solutions.

4.3.12.1. Overview

The Overview tab allows you to configure firewall settings for the selected clients.
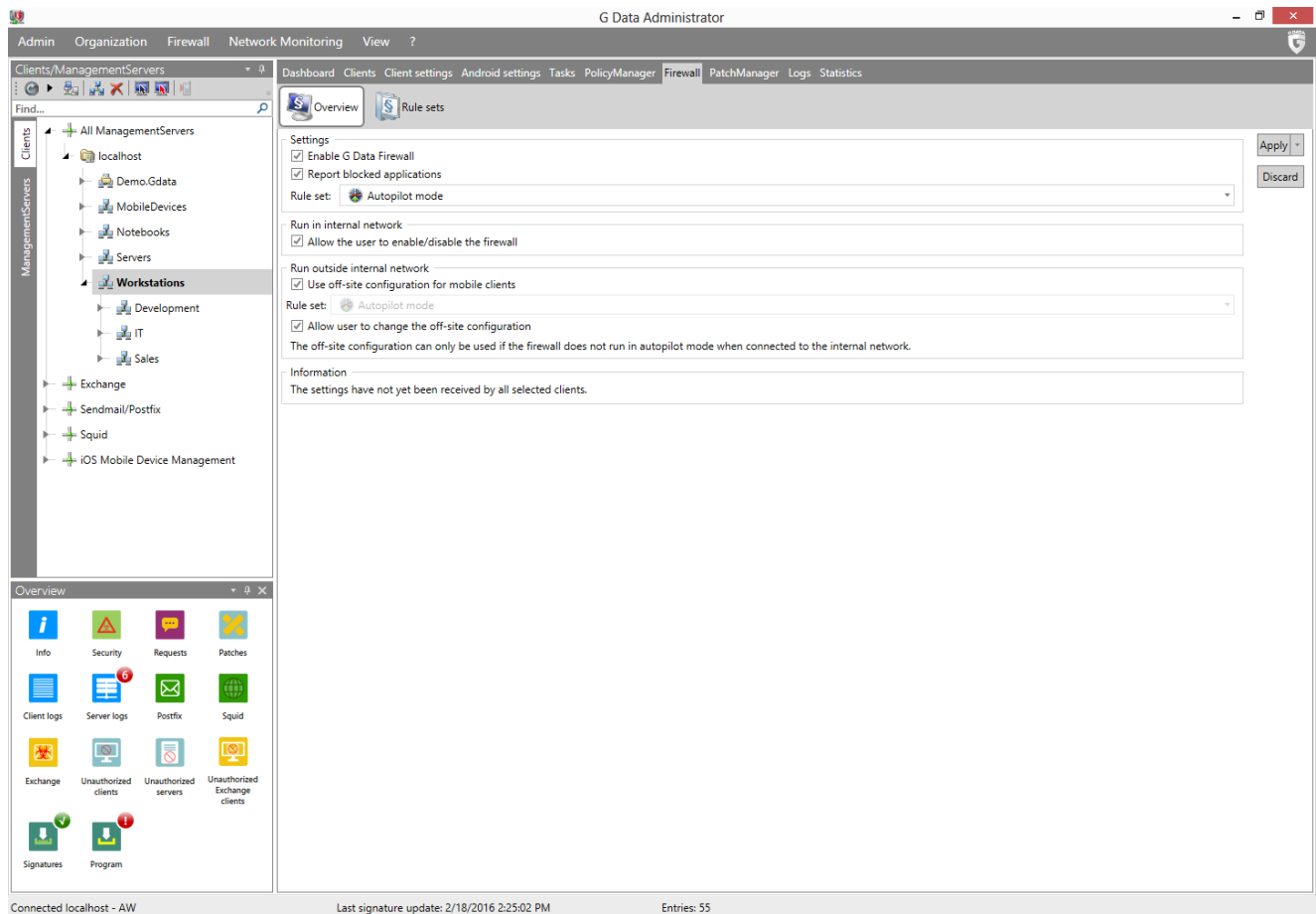
Settings

The Settings section covers general firewall settings:

- **Enable G DATA Firewall**: Enable/disable the firewall.

  Note: From version 14 onwards, clients that do not yet have the firewall component installed, need to be updated to the new version before the firewall can be enabled.

- **Report blocked applications**: If the client computer is connected to G DATA ManagementServer, the system administrator will be notified in the **Security events** module when applications have been blocked by the client firewall.

- **Rule set**: Select the rule set that should be used by the client:

  - **Autopilot mode**: The rules are automatically configured by G DATA and the firewall carries out its tasks in the background, without interrupting the user. In Autopilot mode, the firewall optimizes its rule set autonomously over time.

  - Any of the rule sets that have been created on the **Rule sets** panel.

Run in internal network

Under Run in internal network, define settings that apply when the client is used within the ManagementServer network:

- **Allow user to enable/disable the firewall**: As network administrator, you can allow the user of the client 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.

Run outside internal network

Under Run outside internal network, define settings that apply when the client is used outside the ManagementServer network:

- **Use off-site configuration for mobile clients**: To optimally protect mobile computers whenever they are outside of the G DATA ManagementServer network, the firewall rule set can be automatically replaced by an off-site rule set. As soon as the mobile computer is reconnected to the G DATA ManagementServer network, the regular rule set is automatically restored.

  Note: The off-site configuration can only be used if the firewall is not being operated in autopilot mode when running in the internal network. If a client uses autopilot in the internal network, that setting is also used when the client is outside the internal network.

- **Rule set**: Select the off-site rule set that should be used by the client:

  o **Autopilot mode** (see **Firewall** > **Overview** > Settings).

  o Any of the rule sets that have been created on the Rule sets panel.

- **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 network, the changes made will be replaced with the rules put in place by the network administrator.

4.3.12.2. 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.

The currently selected rule set is listed under **Rule set**. Rule sets can be managed using the New, **Delete**, **Import** and **Export** buttons. Under **Settings**, the following settings can be configured:

- **Name**: The name of the selected rule set.

- **Note**: A description of the selected rule set.

- **Stealth mode enabled**: Block requests to the computer that try to verify a port's accessibility. This makes it difficult for attackers to obtain system information.
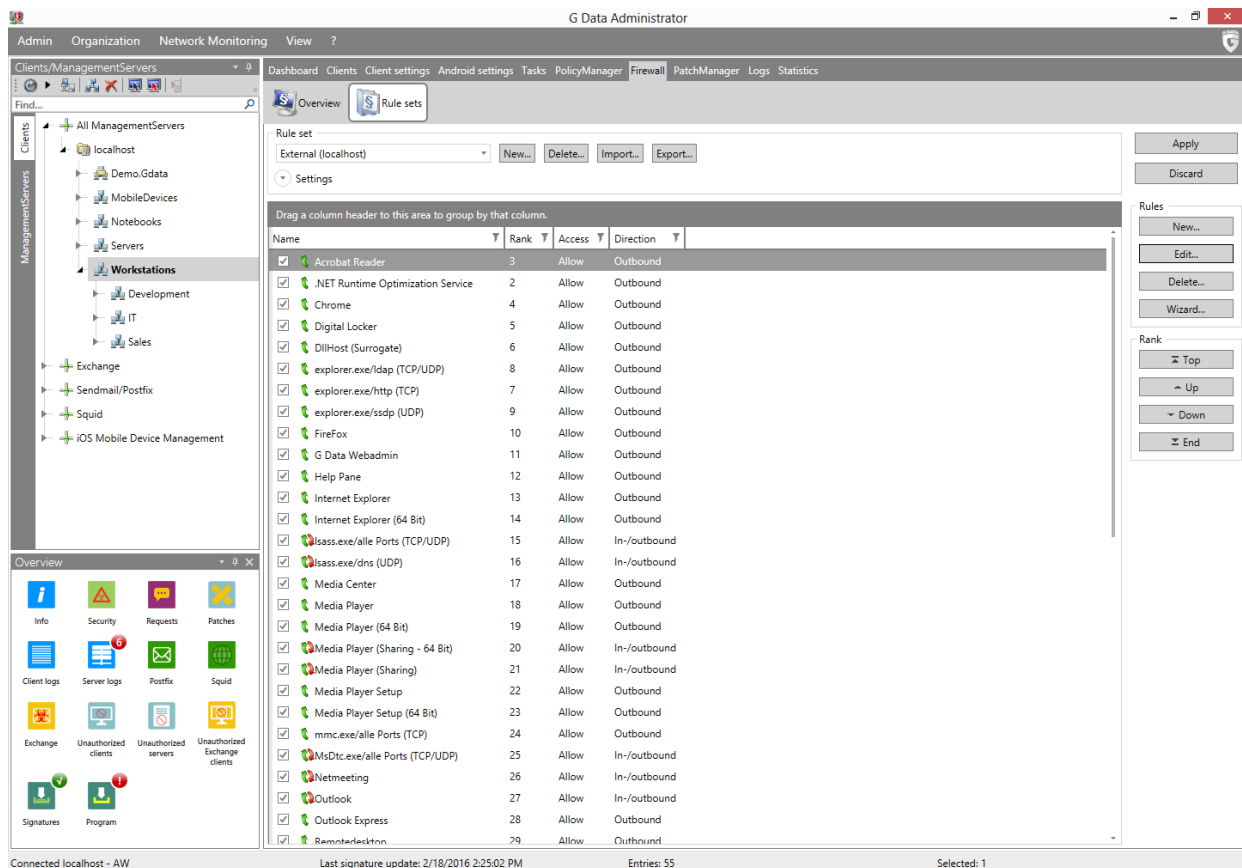
The rules for the currently selected rule set are listed in the lower part of the panel. Under **Rules**, you can **add a new rule/edit an existing rule**, delete a rule or open the **Rule wizard** window. Firewall rules are executed in order of their rank within the rule set. Under **Rank**, you can move the individual rules using the **Top**, **Up**, **Down** and **End** buttons.

New rule set
Enter a **Name** for the rule set and an optional **Note**. Select **Stealth mode enabled** to block requests to the computer that try to verify a port's accessibility.
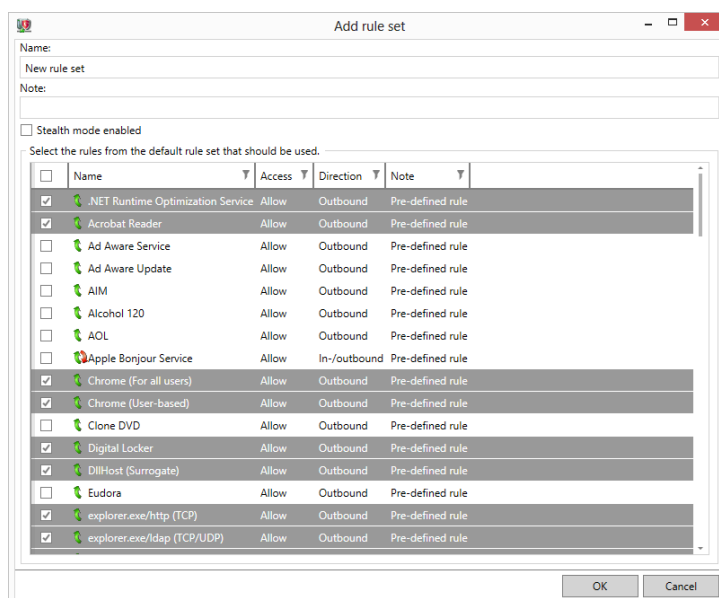
Under **Select the rules from the default rule set that should be used**, pick one or more predefined rules to add to the rule set. After clicking **OK**, the rule set will be shown in the **Rule sets** overview.

New rule/Edit rule

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**: Enable/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**: 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 helps you add rules to the selected rule set or to modify existing rules.
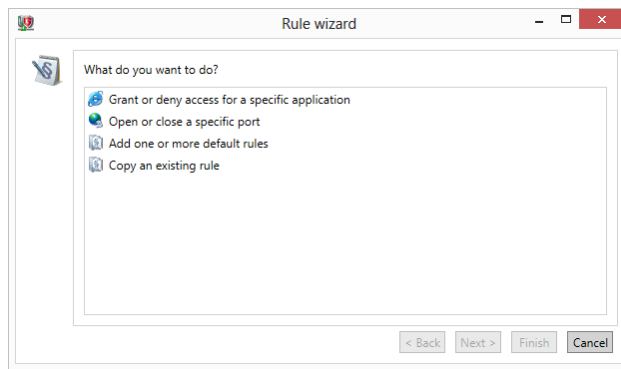
The following actions are available in the Rule wizard:

- **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**: Add rules from the default rule set to the selected rule set.

- **Copy an existing rule**

4.3.13. PatchManager

PatchManager is available as an [optional module](#).

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

4.3.13.1. Status overview

The Status overview panel provides a detailed view of patches and their deployment status within the network. It lists all of the available patches, alphabetically, once for every client. The extensive list lets you check whether clients have been provided with all relevant patches and allows you to directly schedule patch deployment. A set of charts shows at-a-glance information about pending patches and can be used to quickly assess whether there are any important patches that need to be installed.

By default, the list of patches is grouped by **Status**, **Priority**, **Vendor** and **Product**, to quickly assess whether essential patches have been installed yet or not. The default display filter settings exclude full software installers from the list, as well as any blocked entries. Click **Reset all filters** to reset the display filter. Patches that replace a previous patch can be expanded: click the plus sign to display all superseded patches.
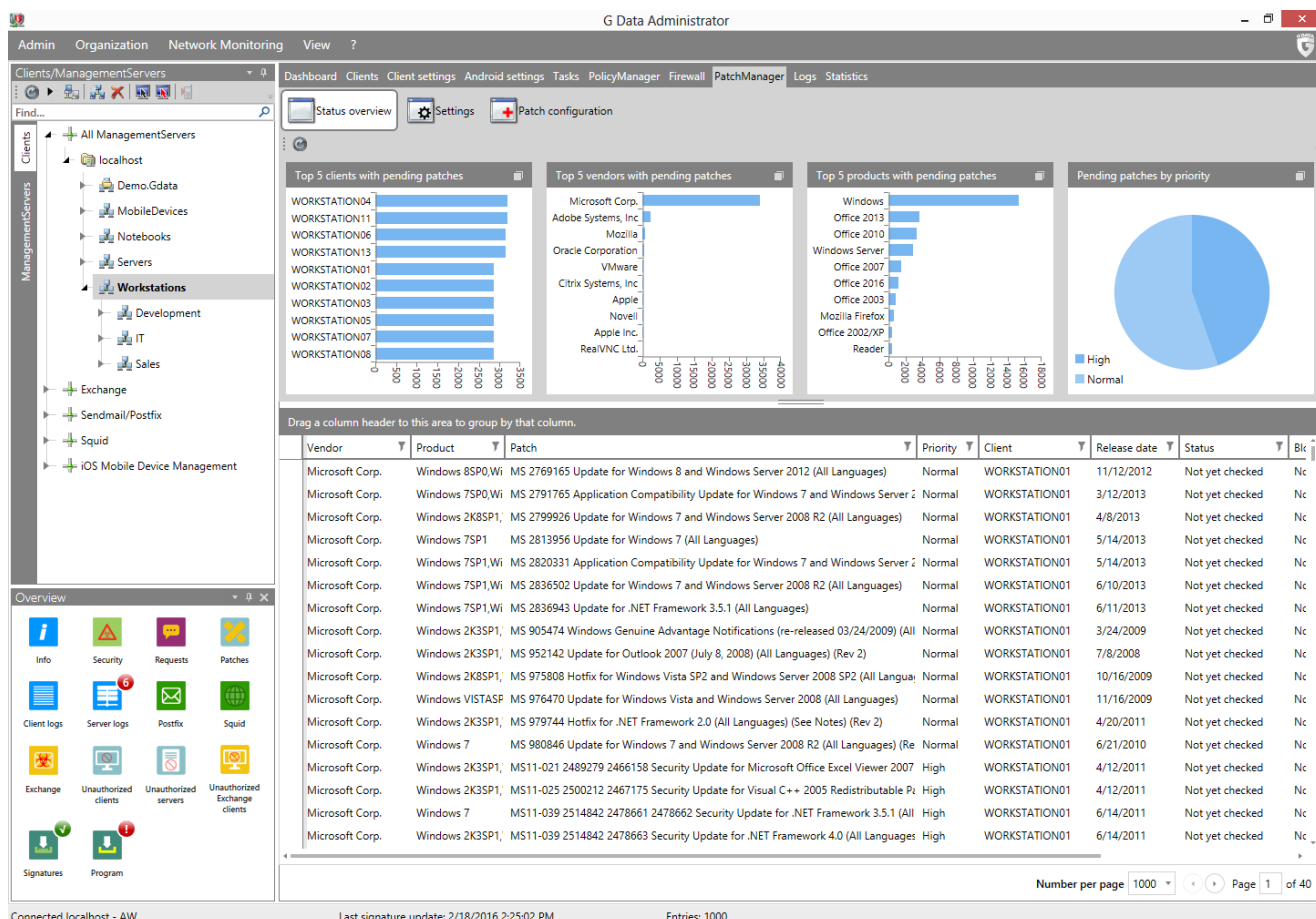
Per patch and client, several types of patching jobs can be planned. Right-click one or more patches and select one of the following options:

- **Check patches for applicability**: Plan a job that checks if the selected patches apply to the selected client(s) using the **Patch applicability job** window.

- **Install patches**: Plan a job that installs one or more patches on the selected client(s) using the **Software distribution** window.

- **Rollback**: Plan a rollback job for patches that have already been deployed to the selected client(s) using the **Rollback** window.

- **Block patches**: Block one or more patches that should not be distributed to clients. Blocked patches will be ignored when carrying out automated applicability and distribution jobs. When manually planning an applicability or distribution job, blocked patches are hidden by default.

- **Unblock patches**: Unblock one or more patches.

- **Properties**: View more information, including a full description and license.

The **Status** column displays the status of every patch and its planned or running patching jobs (e.g. *Scanning* while a job is being carried out or *Not applicable* when the patch does not apply).

4.3.13.2. Settings

The Settings panel controls several options related to patch deployment.

- **Enable PatchManagement**: Enable or disable PatchManager.

- **Mode**: Decide whether PatchManager should run any automated applicability or installation jobs:
  - **Manually**: PatchManager will not run any automated applicability or installation jobs.

- o **Automatically check patches with high priority for applicability**: Whenever a high priority patch is released, PatchManager will automatically run an applicability job on all clients. This saves the effort of planning separate patch applicability jobs.
- o **Automatically install patches with high priority**: Whenever a high priority patch is released, PatchManager will automatically run an installation job on all clients (which installs the patch if it is applicable). Patch deployments can potentially cause compatibility problems. It is recommended to test patches on a non-production system before deploying them to production clients.

- **Allow the user to view and request patches**: Allow end users to view available patches and submit a request for deployment.

- **Allow the user to refuse patch installation**: Allow end users to (temporarily) refuse patch installation. You can select how many refusals are allowed until installation is forced, and how often patch installation should be attempted.
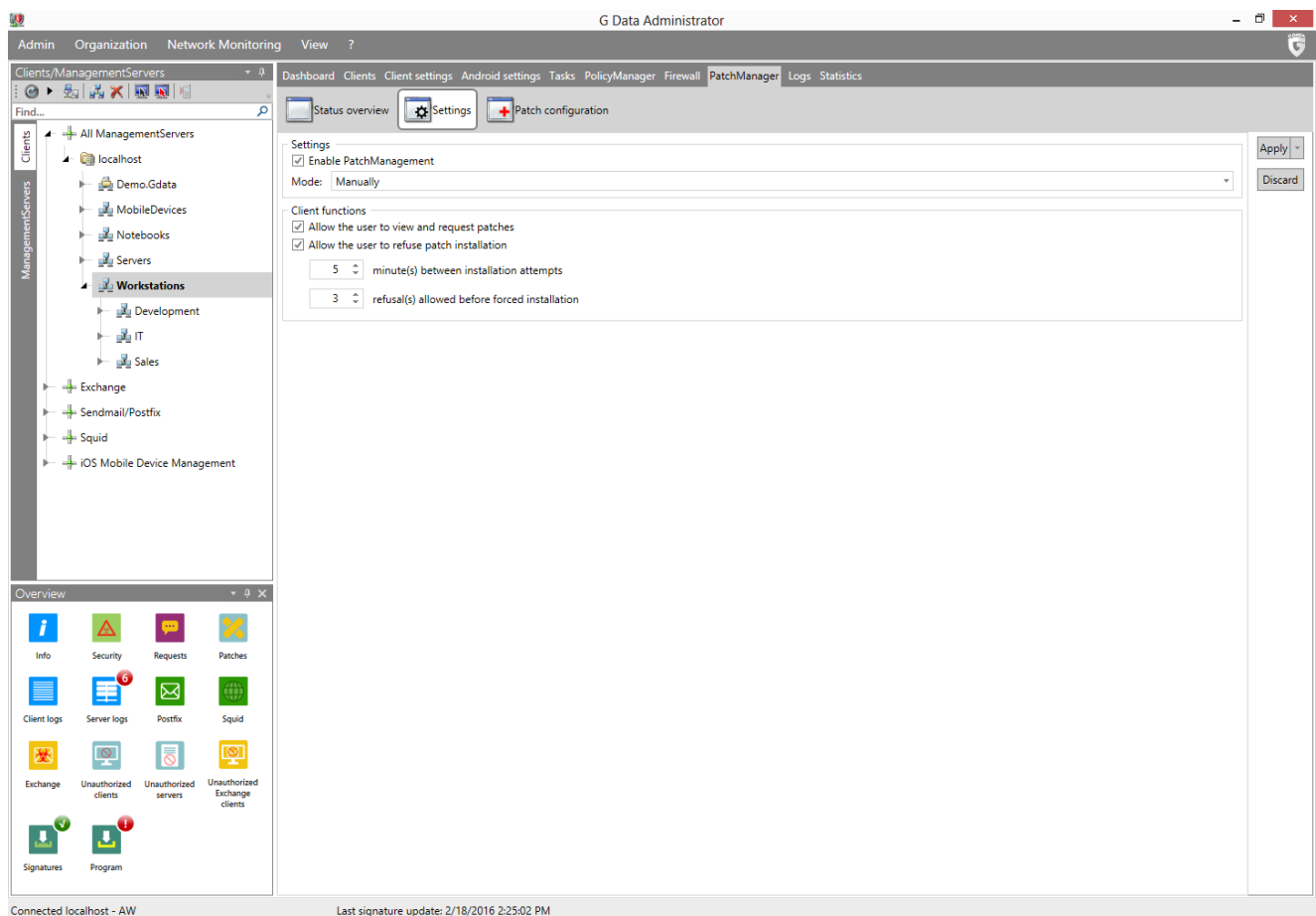
4.3.13.3. Patch configuration

The Patch configuration panel lists all available patches and lets you configure them. A set of charts shows statistics about patches, products, and vendors.

By default, the list of patches is grouped by **Vendor**, **Product** and **Priority**, allowing you to quickly find patches by product. The default display filter settings exclude full software installers from the list, as well as any blocked entries. Click **Reset all filters** to reset the display filter. Patches that replace a previous patch can be expanded: click the plus sign to display all superseded patches.

Per patch, several types of patch jobs can be planned. Right-click one or more patches and select one of the following options:

- **Check patches for applicability**: Plan a job that checks if the selected patch(es) apply to

client(s) using the **Patch applicability job** window.

- **Install patches**: Plan a job that installs one or more patches on client(s) using the **Software distribution** window.

- **Block patches**: Block one or more patches that should not be distributed to clients. Blocked patches will be ignored when carrying out automated applicability and distribution jobs. When manually planning an applicability or distribution job, blocked patches are hidden by default.

- **Unblock patches**: Unblock one or more patches.

- **Properties**: View more information, including a full description and license.
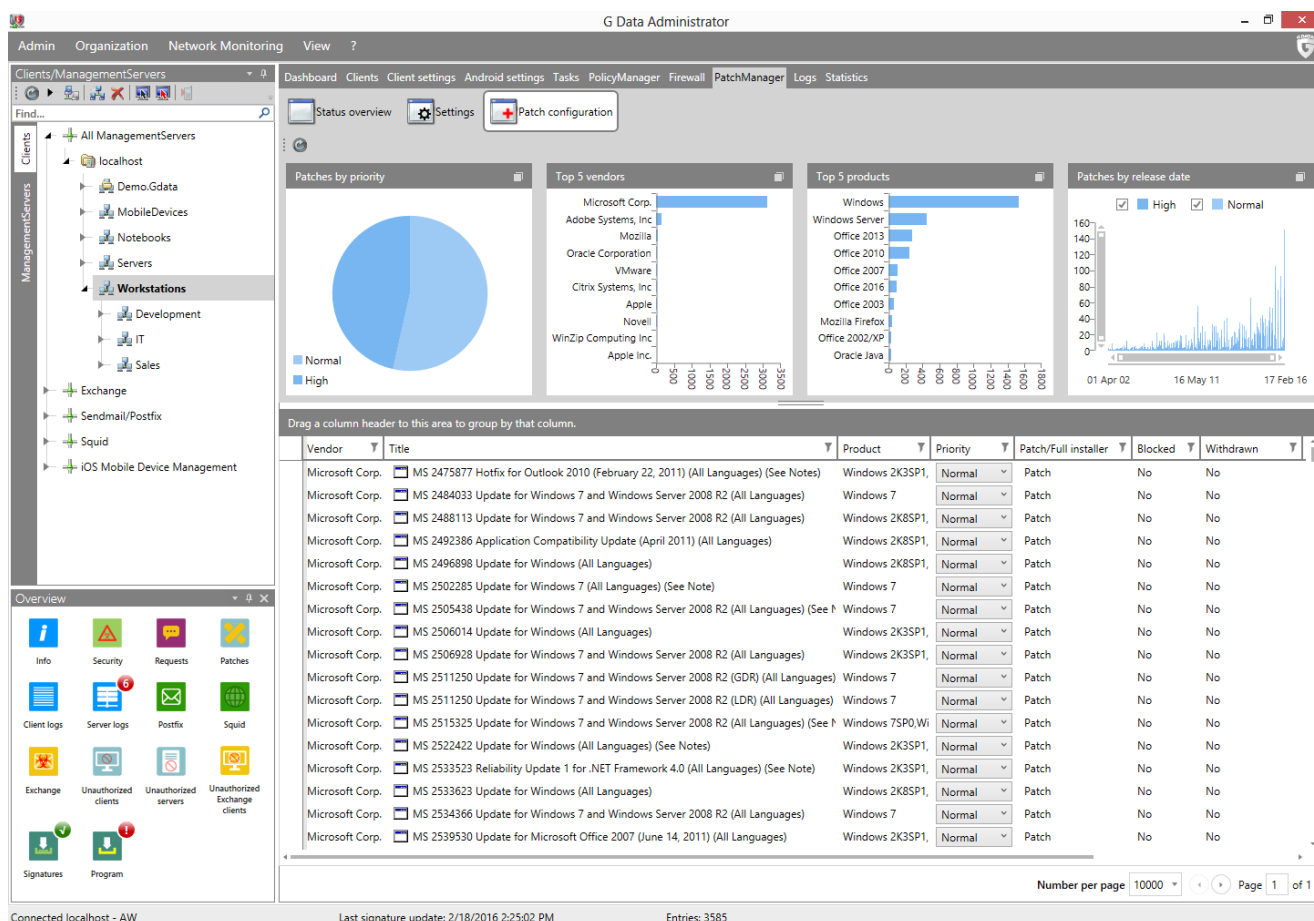
The **Priority** column displays the priority of every patch. The default priority is based on the PatchManager database, but can be edited (**Low**, **Normal**, or **High**).

4.3.14. Logs

The Logs module displays client-side **Security events** such as virus reports and PolicyManager requests, and **Infrastructure logs** such as changed settings and scan job status information.

4.3.14.1. Security events

The Security events panel includes virus results, PolicyManager requests, PatchManager reports, and firewall reports, as well as system messages about installations, reboots, etc. The event type is displayed in the **Status** column (e.g. **Virus found** or **Quarantine: file moved to quarantine**).

If you have configured scan jobs to only log viruses, you can execute virus countermeasures manually by selecting one or more entries from the list and choosing a command from the context menu (right mouse button), the **Security events** menu or the toolbar. Countermeasures available include removing and quarantining infected files.

The **Security events** menu and the right-click context menu offer the following functions:

- **View**: Indicate whether you would like to see all reports, or only a subset of report types:
  - **Hide dependent reports**: If identical reports are available (based on the **Client**, **Reported by** and **File / Mail / Content** fields), you can hide the duplicate entries using this option. Only the most current entry is shown.
  - **Hide read reports**: Hide reports that have already been read.
- **Remove virus from file** (only for virus reports): Attempt to remove the virus from the original file.
- **Move file to quarantine** (only for virus reports): 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 **G DATA Security Labs** 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** (only for virus reports): Deletes the original file on the client.
- **Define monitor exception** (only for monitor reports; only in the context menu): Create a monitor whitelist entry based on the report (see **Client settings** > **Monitor** > **Settings**).
- **Define ExploitProtection exception** (only for ExploitProtection reports; only in the context menu): Create an ExploitProtection whitelist entry based on the report (see **Client settings** > **Monitor** > **ExploitProtection**).
- **Revoke keyboard authorization**: Revokes the authorization for a keyboard that was detected by USB Keyboard Guard and authorized by the end user.

- **Quarantine: clean and move back** (only for quarantine reports): 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** (only for quarantine reports): 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 to G DATA Security Labs** (only for quarantine reports): 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** (only for quarantine reports): Delete the selected report and remove the file from the quarantine.

- **Add URL to whitelist** (only for **Web content control** reports): Add the requested URL to the global whitelist.

- **Add URL to blacklist** (only for **Web content control** reports): Add the requested URL to the global blacklist.

- **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.

- **Clean up reports**: If identical reports are available (based on the **Client**, **Reported by** and **File / Mail / Content** fields), you can delete the duplicate entries using this option.

  The option Clean up reports only applies to reports that are currently shown. If a filter is active, reports that are not shown are not considered for cleanup. If there is more than one page of reports, only reports on the current page are considered for cleanup.

- **Export reports** (only in the context menu): Export the selected report(s) or the entire list as an XML file.

- **Mark as read** (only in the context menu): Mark the selected reports as read.

- **Mark as unread** (only in the context menu): Mark the selected reports as unread.

- **Details/Actions** (only in the context menu): Some events 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 and select Details/Actions. In the **Distribute software (rollback)** window you can then directly plan a rollback job, without having to open the **PatchManager** module to select the patch and client.

The toolbar of the Security events tab offers the following options and filter settings:

- **Refresh**
- **Delete**
- **Print**
- **Print preview**
- **Remove virus**
- **Move to quarantine**
- **Delete file**
- **Move file back from quarantine**
- **Clean file & move back from quarantine**
- **Hide dependent reports**
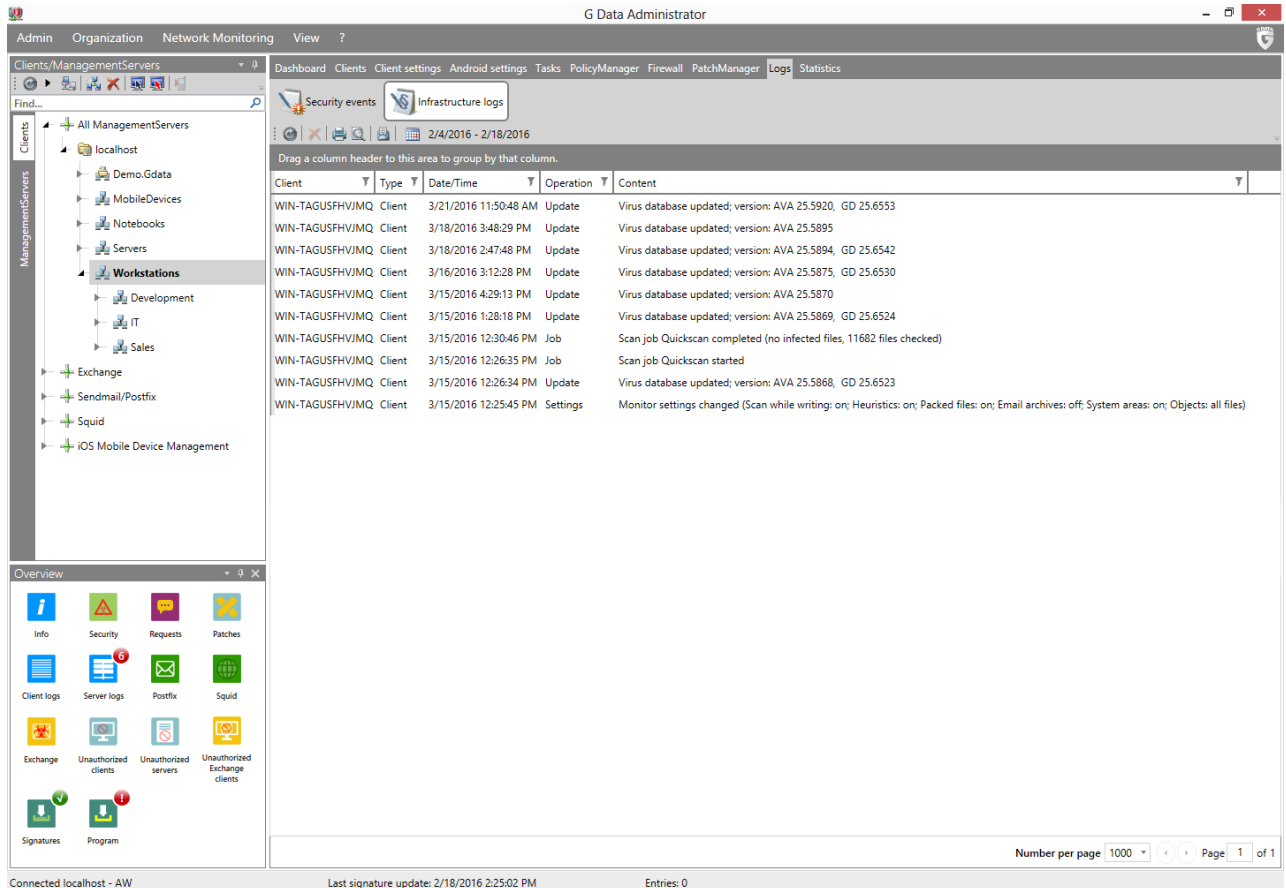
    🖨 **Hide read reports**

    📅 **Time frame**

4.3.14.2. Infrastructure logs

The Infrastructure logs panel displays client status information such as scan job status updates, virus signature updates and changes to settings.

The right-click context menu offer the following functions:

- **Refresh**
- **Delete**
- **Mark as read**: Mark the selected reports as read.
- **Mark as unread**: Mark the selected reports as unread.
- **Export**: Export the selected report(s) or the entire list as an XML file.

The toolbar of the Infrastructure logs tab offers the following options and filter settings:

  🔄 **Refresh**

  ❌ **Delete**

  🖨 **Print**

  🔍 **Print preview**

  🖨 **Hide read reports**: Hide reports that have already been read.

  📅 **Time frame**

4.3.15. Logs (iOS)

When you have selected one or more iOS clients on the **Clients** panel, the Logs module only displays details pertaining to the selected iOS client(s). Reports include status information about the deployment of profiles as well as anti-theft actions.

- **Status**: Report status.
- **Client**: Device name.
- **Date/Time**: Report timestamp.

Right-click a report and select **Delete** to remove it from the list.
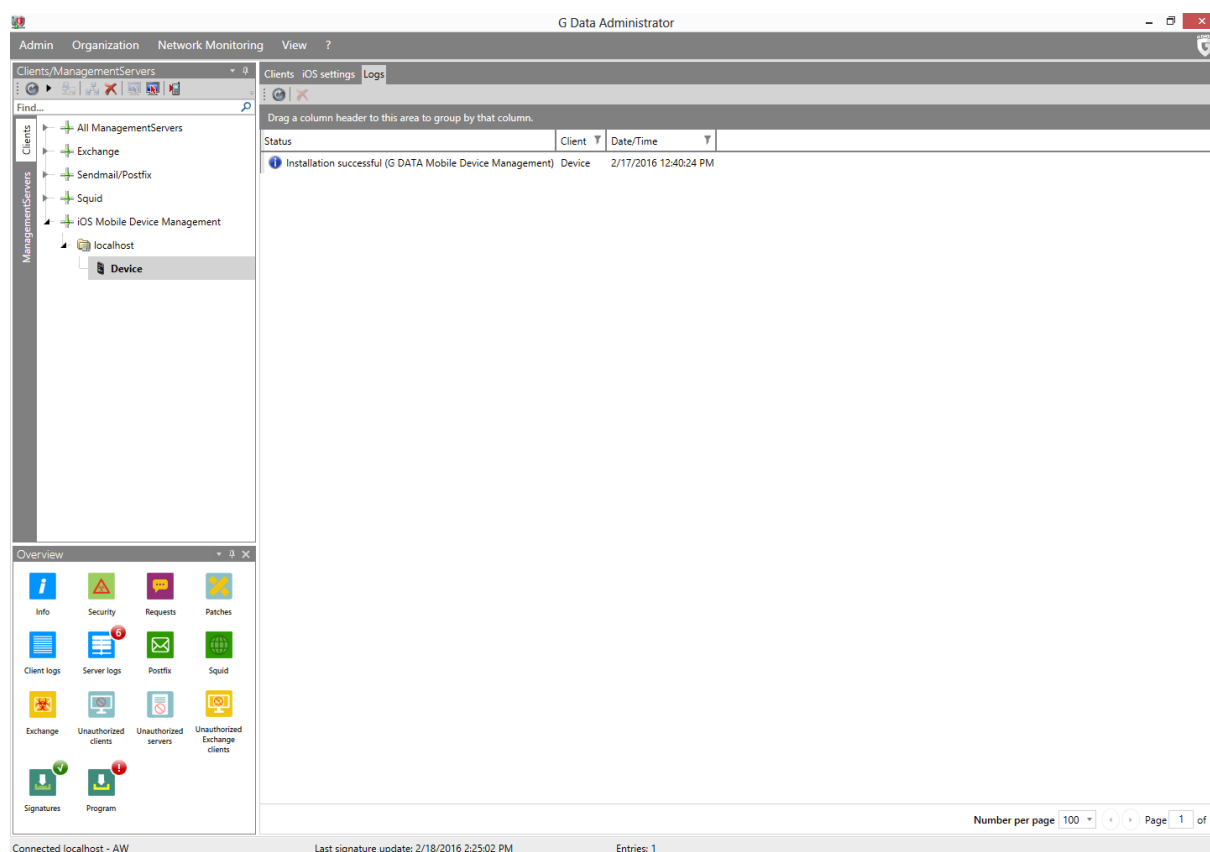
4.3.16. Statistics

In the Statistics module, you can check statistical information about virus occurrences and client/Exchange Server email 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** (not available if an Exchange server has been selected), the **Detection method**, the **Virus hit list** and the **Hit list of neutralized infections**.
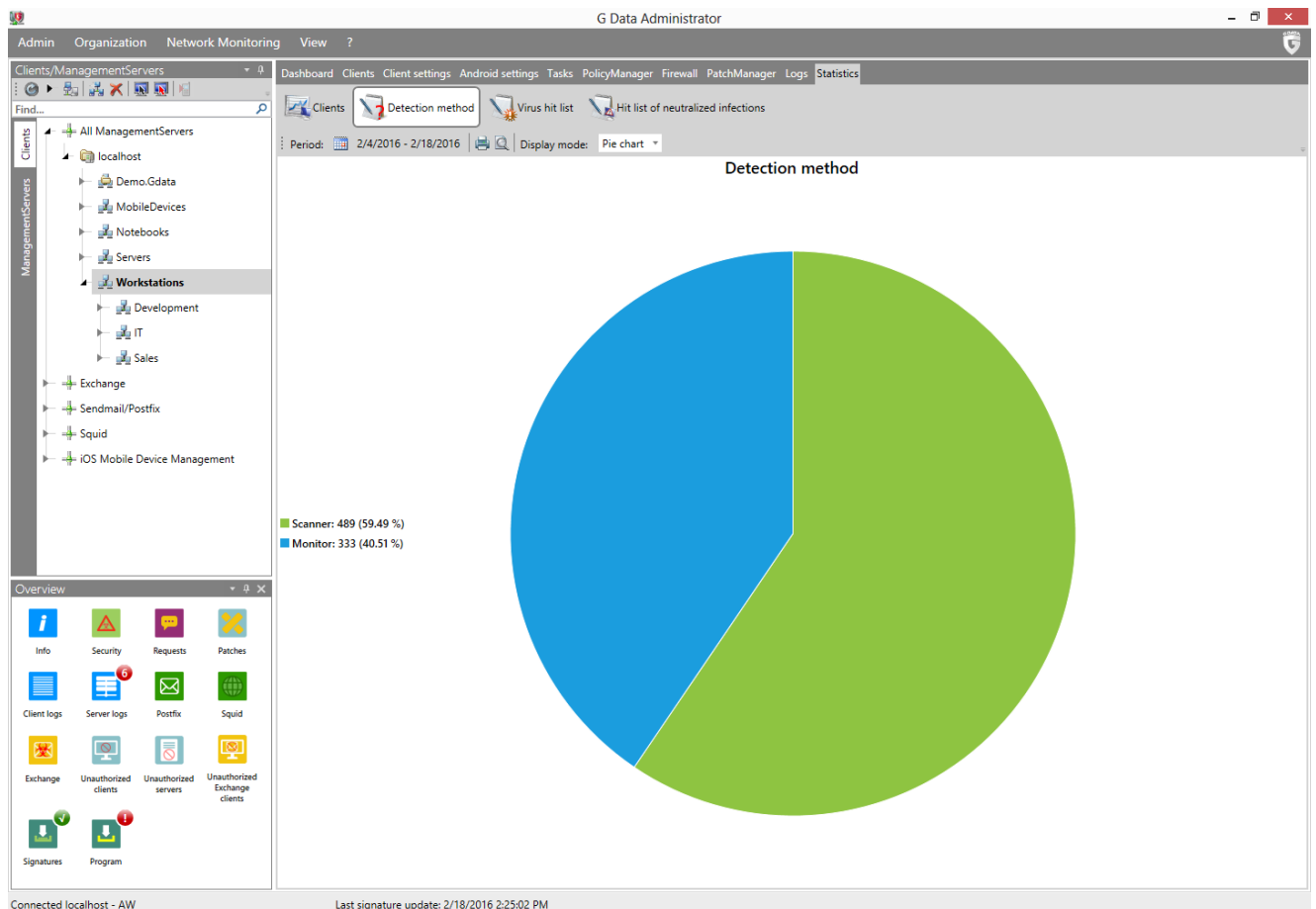
4.4. Server modules

The server modules can be used to configure the server that has been selected on the **ManagementServers** tab of the **Clients/ManagementServers** panel.

4.4.1. Servers

The Servers module offers server management functions, such as version and status information, subnet server management, user management and logs.

4.4.1.1. Overview

The Overview panel can be used to check on server status information and to install and manage subnet servers. It displays the following server properties:

- **Name**: The server name.
- **Type**: The server type (**Main server**, **Subnet server**, **Secondary server**).
- **Server**: The name of the governing ManagementServer (only for subnet servers and secondary servers).
- **Number of clients**: The number of clients currently assigned to the selected server.
- **Last access**: The timestamp of the last synchronization with the main ManagementServer (only for subnet servers).
- **Status as per**: The last signature update attempt.
- **Version**: Version number and date.
- **Status**: Server status information, such as its update status.

- **Program update**: If an update is available for a subnet server, the status is displayed here.
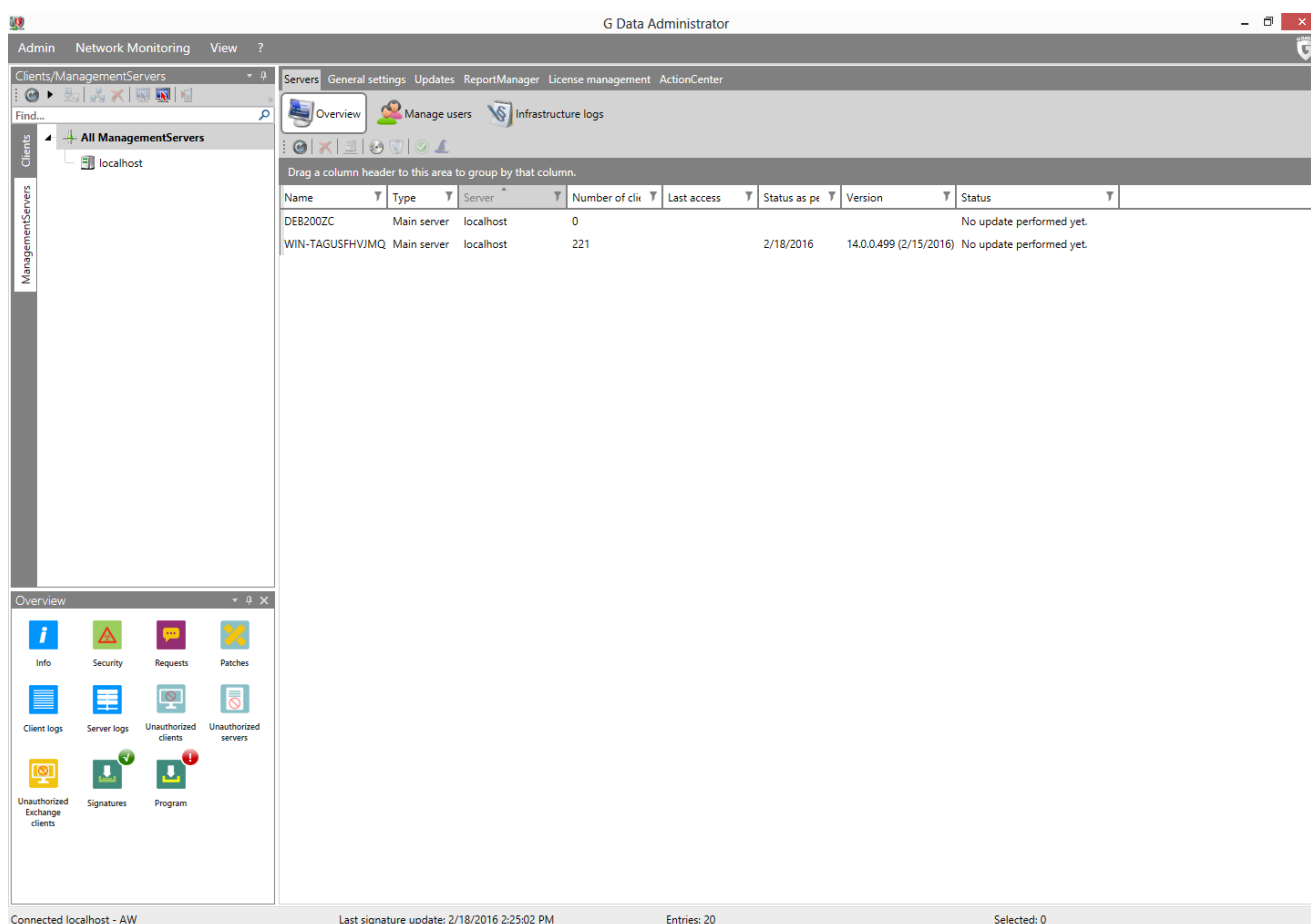
The toolbar and the right-click context menu contain the following options:

- **Refresh**
- **Server setup wizard**
- **Delete**: Remove one or more subnet server(s) from the list. This does not remove the actual software from the subnet server.
- **Synchronize** (context menu only): Initiate a manual synchronization of the selected subnet server(s).
- **Assign clients**: Assign existing clients or groups to subnet servers that 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 **Clients/ManagementServers panel**. That means that clients that have been assigned to different subnet servers can still be grouped together
- **Install 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. A remote subnet server installation is subject to the same prerequisites as a **remote installation of G DATA Security Client**. Subnet servers use Microsoft SQL Server 2014 Express, which does not support Windows Vista and Windows Server 2008/2003. On such systems, subnet servers can be installed through the subnet server option of the **local installation** of G DATA ManagementServer.
- **Uninstall server**: Initialize a remote deinstallation of the selected subnet server, which can be tracked using the **Installation overview** window. A remote deinstallation can only be carried out on authorized subnet servers.

- **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 **Install subnet server** are automatically authorized. Only locally installed subnet servers and subnet servers that have been upgraded from version 12 or earlier need to be authorized manually.

- **Permit program update** (context menu only): Subnet servers with ManagementServer version 12 require a manual installation of a database server, before they can be updated to version 14. On such systems, install Microsoft SQL Server 2014 Express (Windows Server 2008 R2/Windows 7 and newer) or Microsoft SQL Server 2008 R2 Express (Windows Server 2003/2008/Windows Vista) first, then use this option to permit the program update. After the update, use GdmmsConfig.exe on the subnet server to configure the connection to the database. More information can be found in the Reference Guide.

- **Properties** (context menu only): Display properties for the selected server, including the version of the ManagementServer, virus signatures and client program files.

Server setup wizard

The Server setup wizard lets you configure some of the most important settings of G DATA ManagementServer. It is automatically run the first time you start G DATA Administrator, but can also be started afterward under **Servers** > **Overview** and through the **Admin** menu.
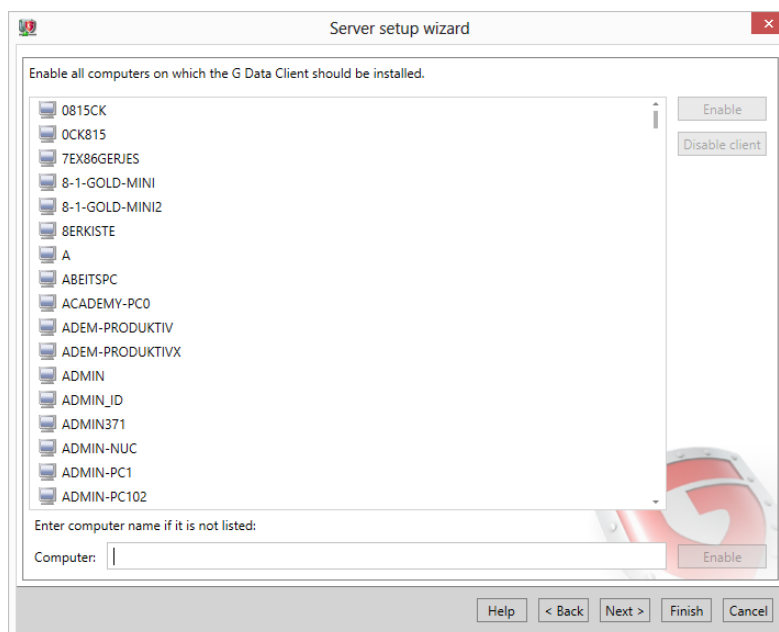
All clients that are to be managed by the G DATA software must first be "enabled". To do this, highlight the clients to be enabled and click the **Enable** button. Some computers may not be included in the list (e.g. because they have not been switched on for a long time or have not set up File and Printer 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 **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.

The next wizard steps help you configure some of the most commonly used settings:

- **Internet update**: Configure virus signature and program file updates. More information can be

found in the Updates module.

- **Email notification**: Configure mail server settings, email groups and alarm notifications. More information can be found under **General settings** > **Email**.

- **Settings for mobile devices**: Configure mobile device management for Android. More information can be found under **General settings** > **Android**.

- **Setting for access to G DATA ActionCenter**: ActionCenter credentials are required to enable iOS device management and network monitoring. More information can be found in the **ActionCenter** module.

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.

4.4.1.2. Manage users

As system administrator, you can authorize additional users to configure G DATA ManagementServer through G DATA Administrator. Click **Add**, then enter the **User name**, the **Account type** (**Integrated authentication**, **Windows user**, **Windows user group**), the **Permissions** for this user (Read only, Read/Write, Read/Write/Restore backups) and enter a **Password**.
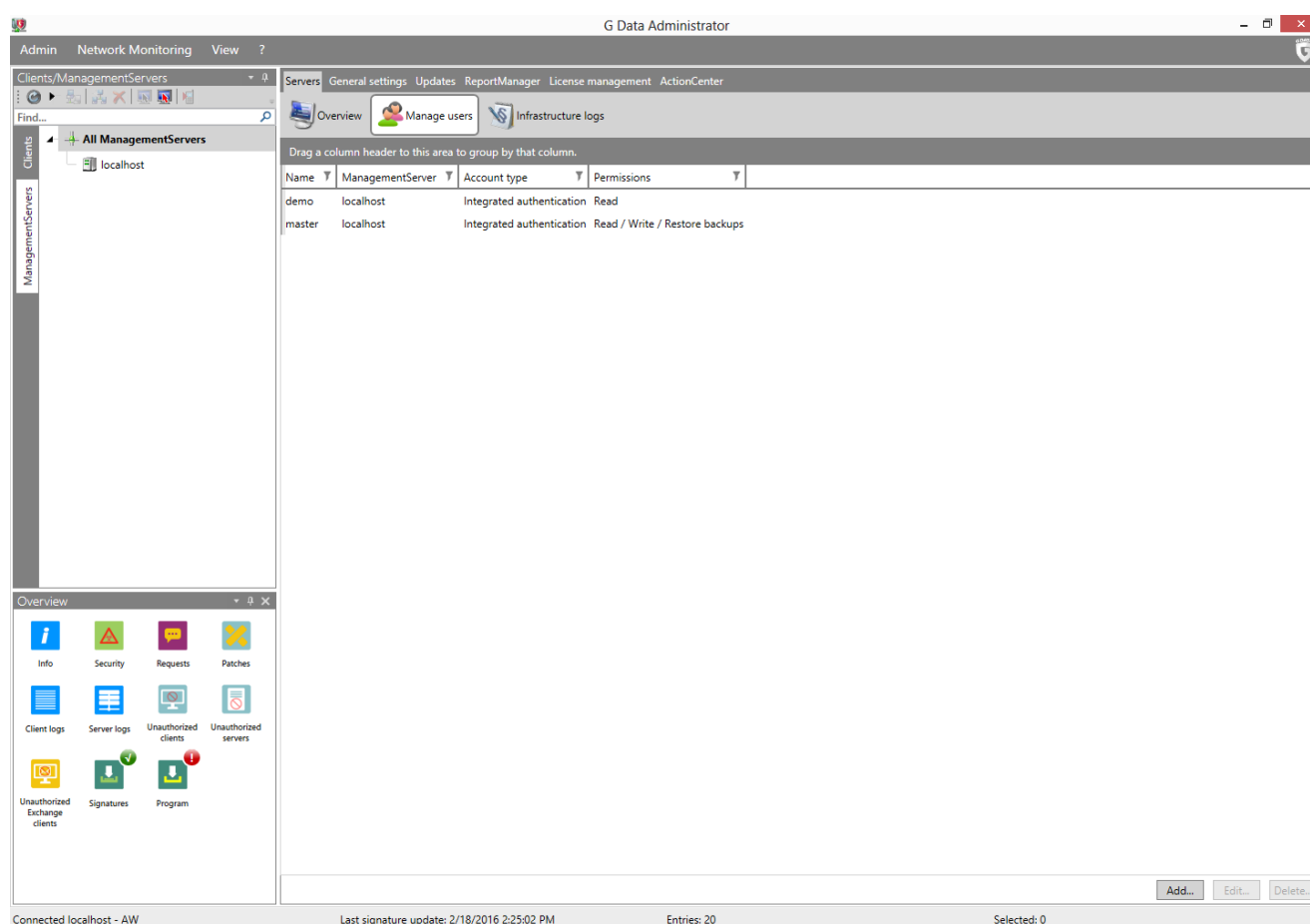
4.4.1.3. Infrastructure logs

The Infrastructure logs panel displays server status information such as signature update and program file update information. The toolbar and context menu options are identical to those in the client module **Logs** > **Infrastructure logs**.

4.4.2. General settings

The General settings module can be used to configure several general server settings, such as subnet server and client synchronization, backup paths, email server and Android mobile device management settings.

4.4.2.1. Cleanup

The Cleanup settings allow you to configure whether various items should automatically be deleted after a specified period of time:

- o **Automatically delete infrastructure logs**: Delete infrastructure logs that are older than the set number of days.
- o **Automatically delete scan logs**: Delete scan log files that are older than the set number of days.
- o **Automatically delete security events**: Delete security reports that are older than the set number of months.
- o **Automatically delete report history**: Delete generated ReportManager reports that are older than the set number of months.
- o **Automatically delete clients following inactivity**: Delete clients that have not logged on for a set number of days.
- o **Automatically delete patch files**: Delete patch files that have not been used for more than the set number of days.
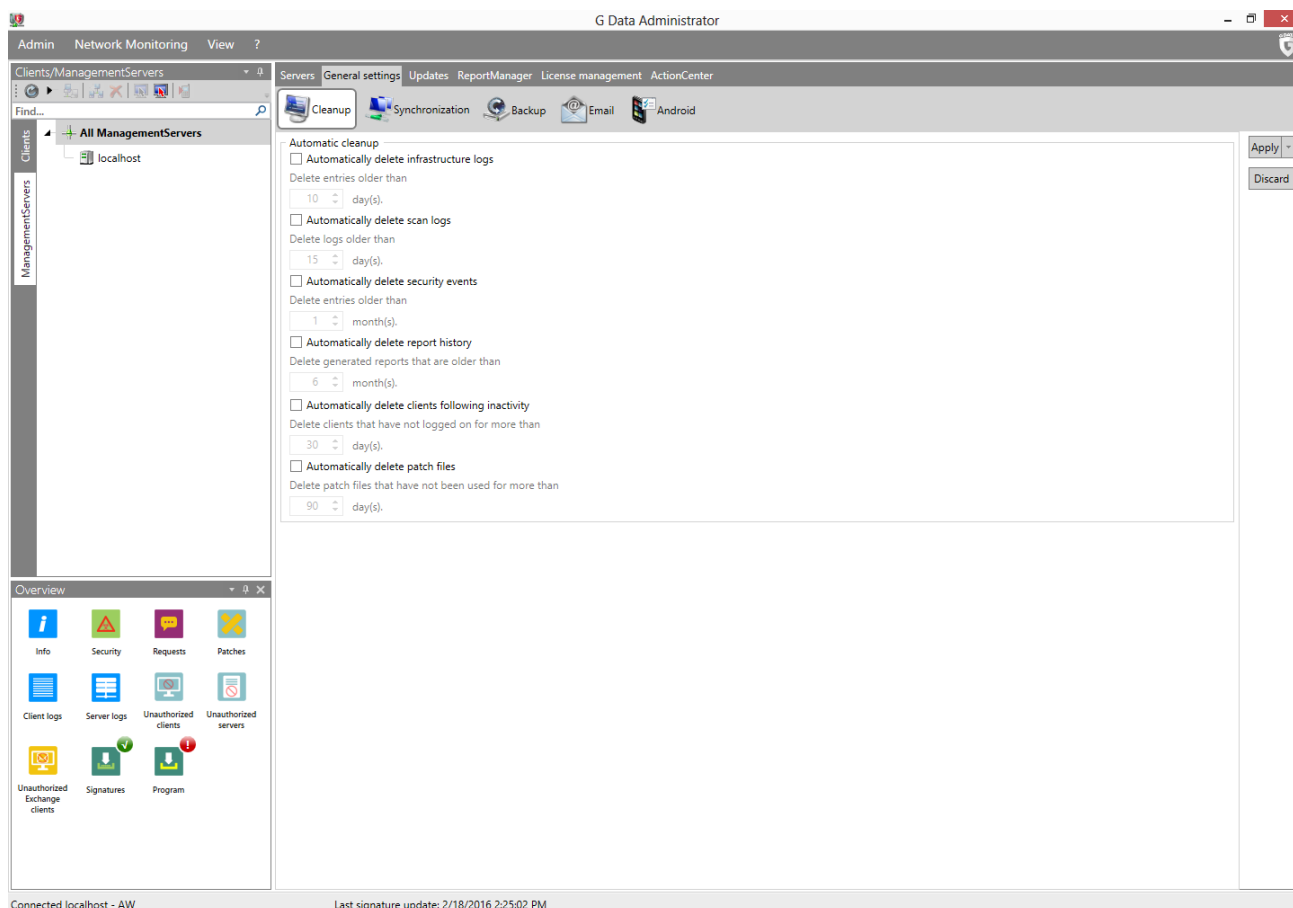
4.4.2.2. Synchronization

In the Synchronization area, you can define the synchronization interval between the ManagementServer and clients, subnet servers and Active Directory:
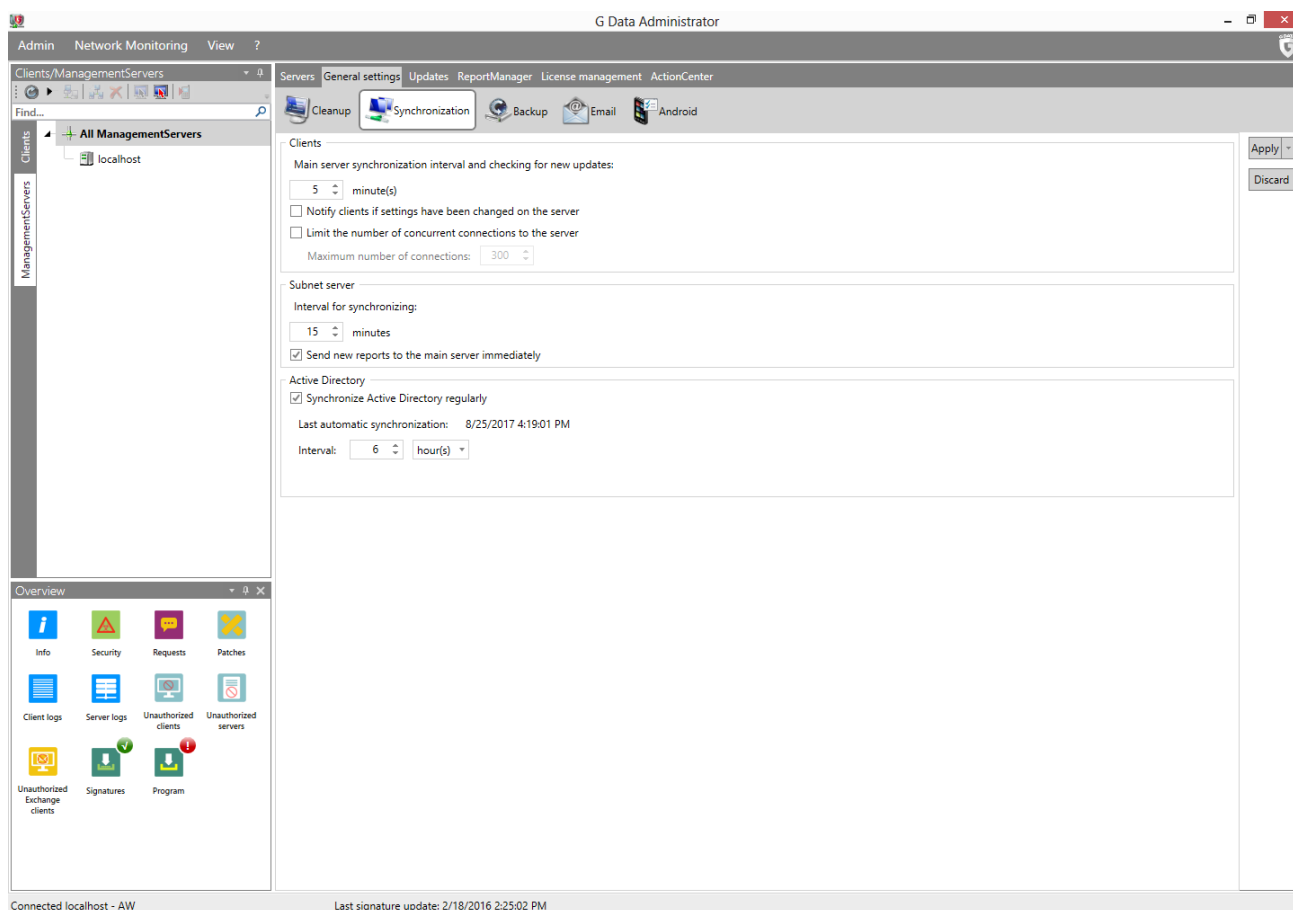
- **Clients**

  o **Main server synchronization interval and checking for new updates**: Enter the time interval in which the clients connect to the ManagementServer to check for new updates or settings. The default value is five minutes.

  o **Notify client if settings have been changed on the server**: Tick this setting to notify clients immediately of new settings, regardless of synchronization interval.

  o **Limit the number of concurrent connections to the server**: Specify how many clients can simultaneously connect to the ManagementServer. The number of Clients depends on the specifications of the server and network infrastructure. If you are experiencing performance issues, reducing the number may improve server performance.

- **Subnet server**

  o **Interval for synchronizing**: Define the interval for synchronization between main ManagementServer and subnet server(s).

  o **Send new reports to the main server immediately**: Enable this option to transfer new reports to the main server immediately, regardless of the synchronization interval.

- **Active Directory**

  o **Synchronize Active Directory regularly**: Enable regular synchronization between ManagementServer and Active Directory. Synchronization is only carried out if at least one group has been assigned an Active Directory Organizational Unit.

  o **Interval**: 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.

4.4.2.3. Backup

Backup is available as an optional module.

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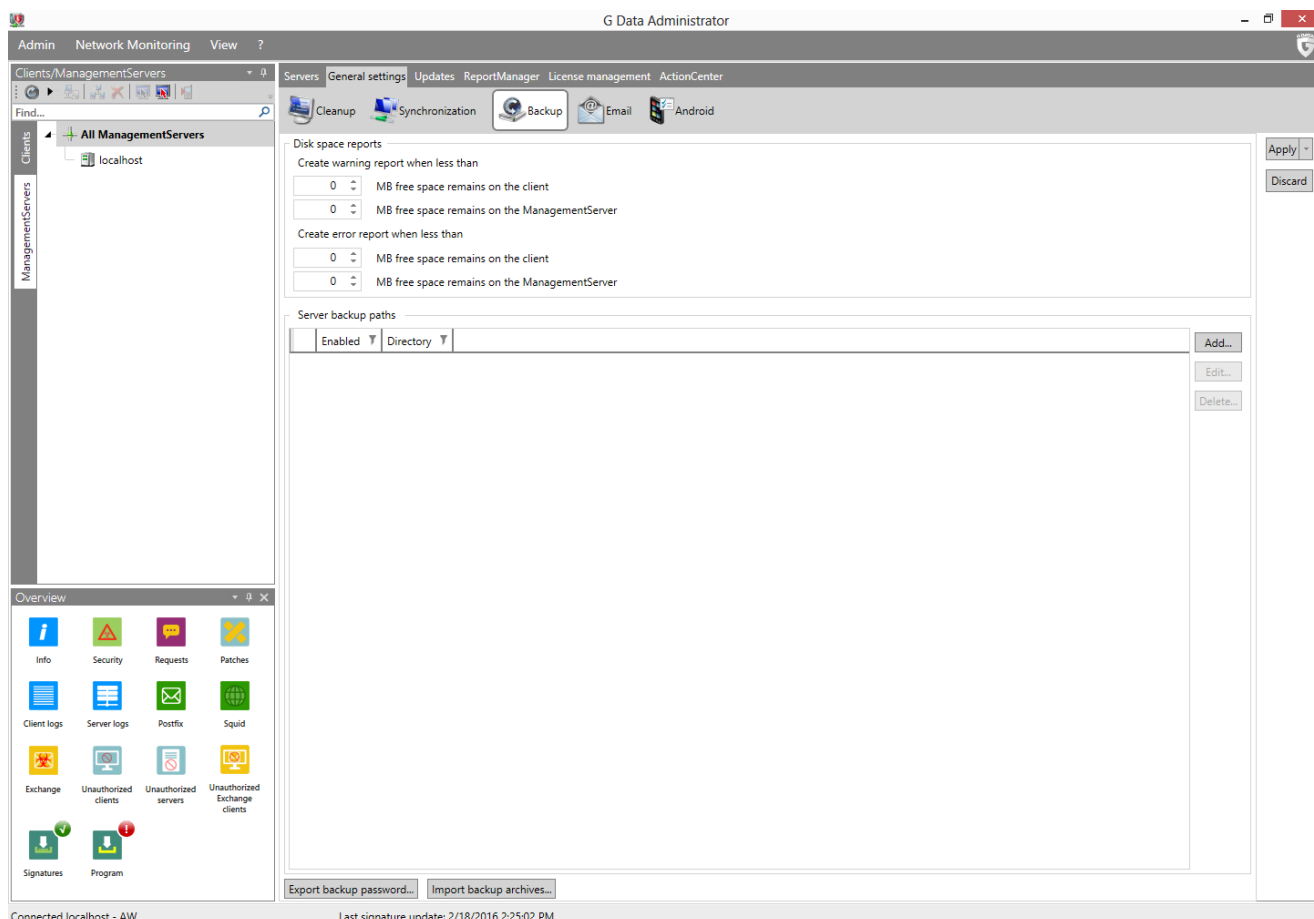
Under **Server backup paths** a path can be entered where all backups being generated are stored. If no path is entered here, all backups are stored under C:\ProgramData\G Data\AntiVirus ManagementServer\Backup or C:\Documents and Settings\All Users\Application Data\G Data \AntiVirus ManagementServer\Backup.

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.

4.4.2.4. Email

G DATA ManagementServer can automatically send alarm notifications when certain events occur. Enable email notification by selecting the appropriate **Reports** (**Virus results**, **Permission 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. After selecting a recipient, click **Trigger test alarm** to send a test alarm.
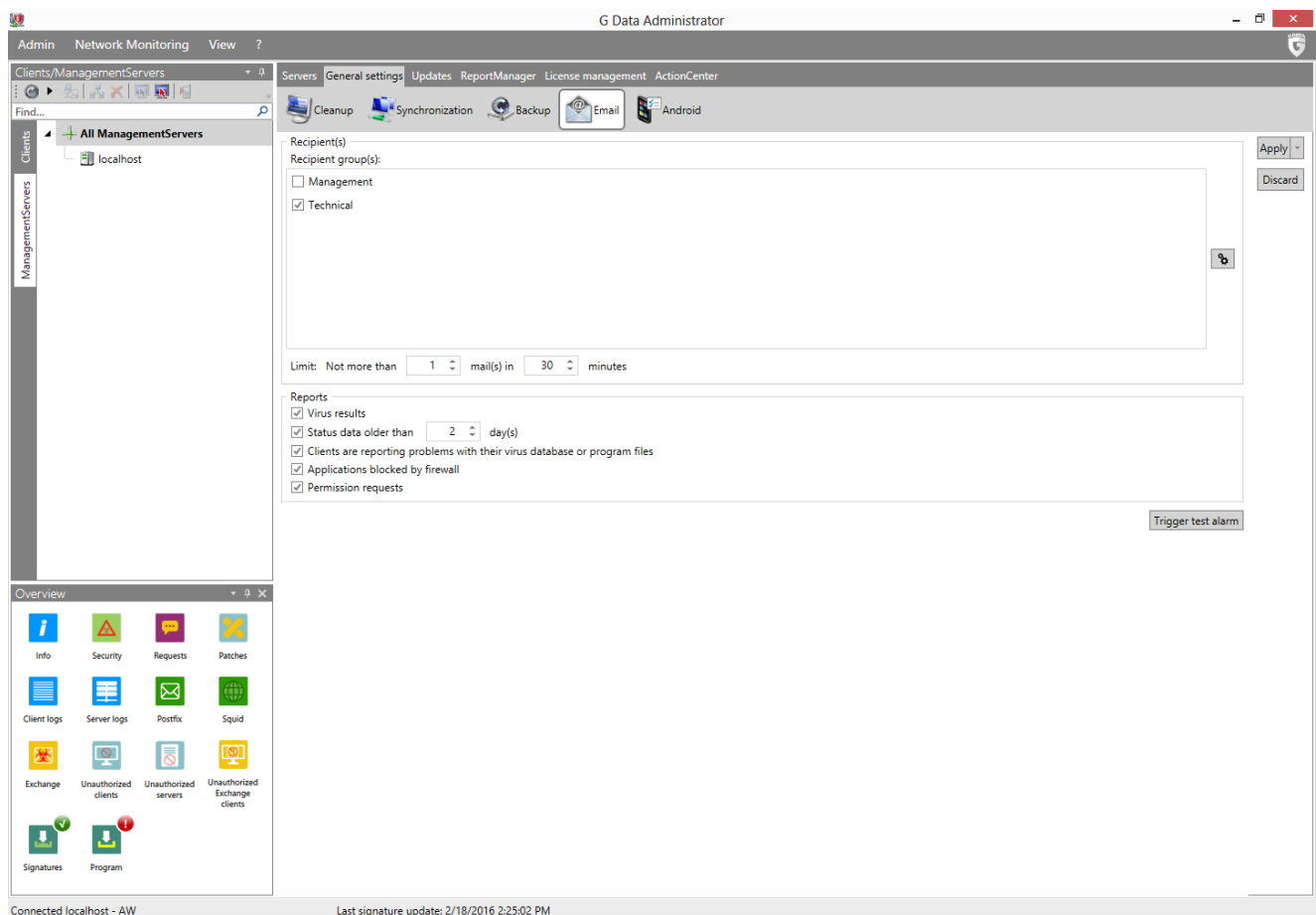
Click the cogs icon (⚙) to open the **Email settings** window to define mail groups and mail server authentication.

Email settings

Enter the **SMTP server** and **Port** (normally *25*) that G DATA ManagementServer should use to send email. In addition a (valid) sender address is required so emails can be sent. 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.
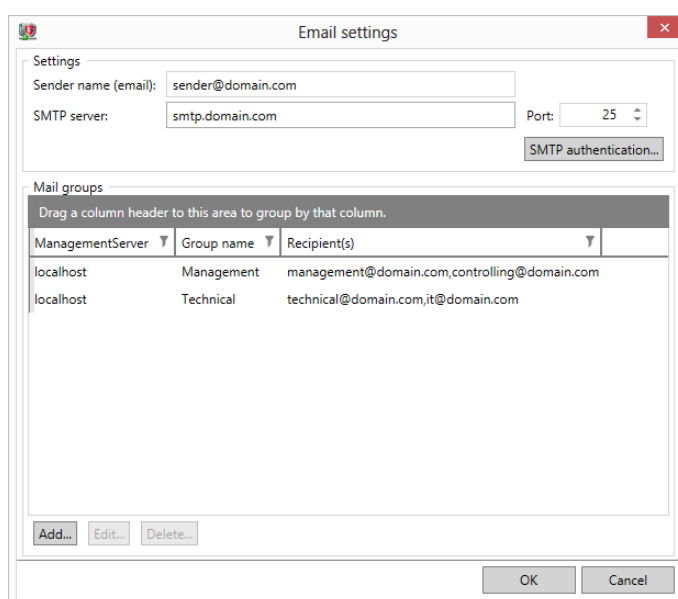
Under **Mail groups** you can manage recipient lists, such as Management or Administrators.

4.4.2.5. Android

The Android panel features settings for the authentication of Android clients as well as Firebase Cloud Messaging.

Under **Authentication for Android clients**, enter a **Password** with which Android 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** (Server key) of your Firebase Cloud Messaging account. Free accounts for this push notification framework can be registered at **firebase.google.com**. Consult the Reference Guide for more information about Firebase Cloud Messaging.
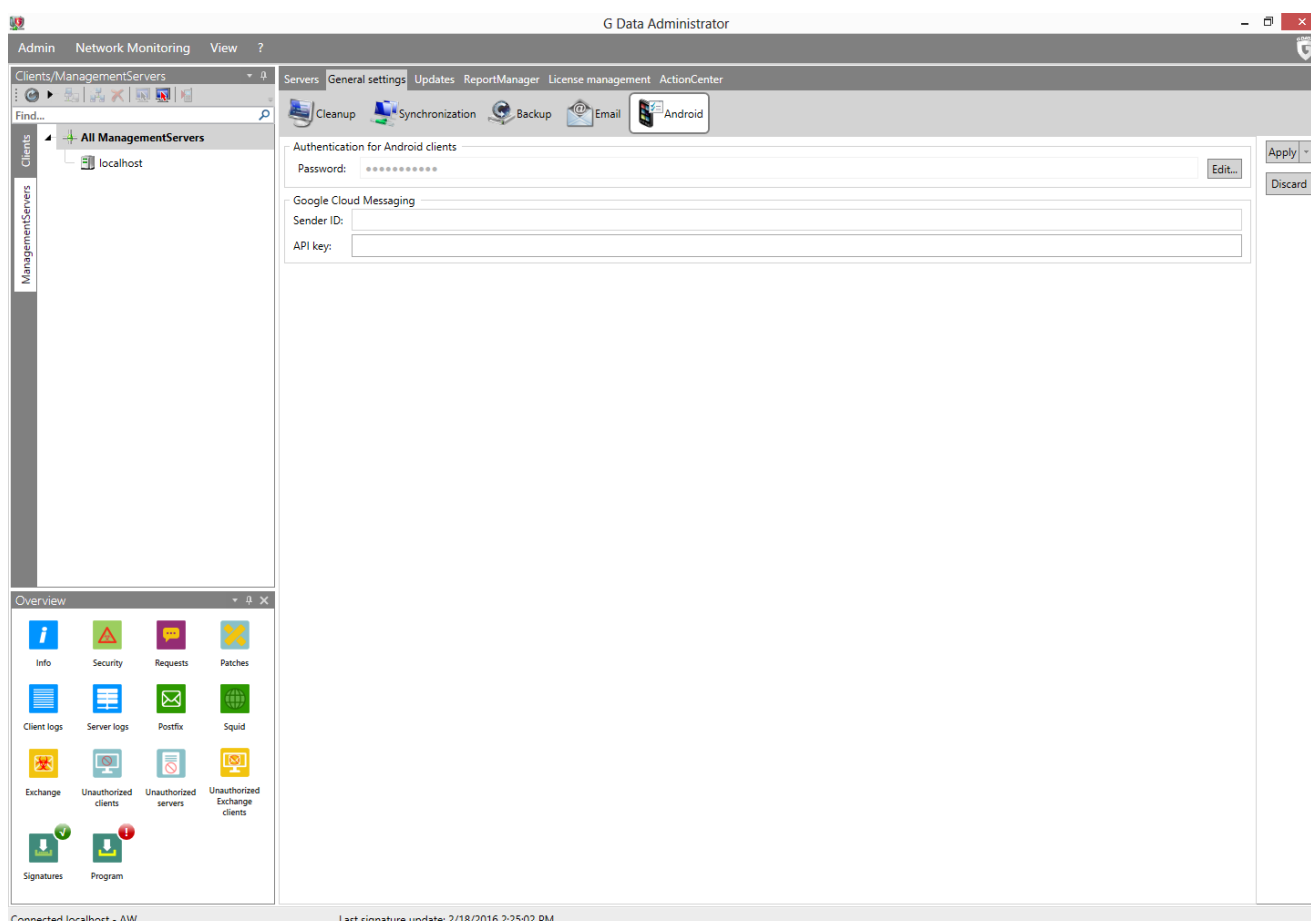
4.4.3. Updates

All clients have their own local copy of the virus signature database, so that virus protection is also guaranteed when no connection to the G DATA ManagementServer or the Internet is available. Updating virus signatures (as well as program files) 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. The Updates module lets you configure this process. Subsequent distribution of the updates to the clients can be configured under **Client settings** > **General** > **Updates**.

4.4.3.1. Signature updates

On the Signature updates panel, you can configure the process of downloading signature updates from the G DATA update server to G DATA ManagementServer.

The following information and settings are available under **Status**:

- **Version engine A**: The current version of the virus signatures for engine A on G DATA

ManagementServer.

- **Version engine B**: The current version of the virus signatures for engine B on G DATA ManagementServer.

- **Last execution**: Timestamp for the last execution of the virus signature update process.

- **Status**: The status of the virus signature update process.

- **Update status**: Update the **Status** field.

- **Run update now**: Carry out an immediate update of the virus signature database on G DATA ManagementServer.
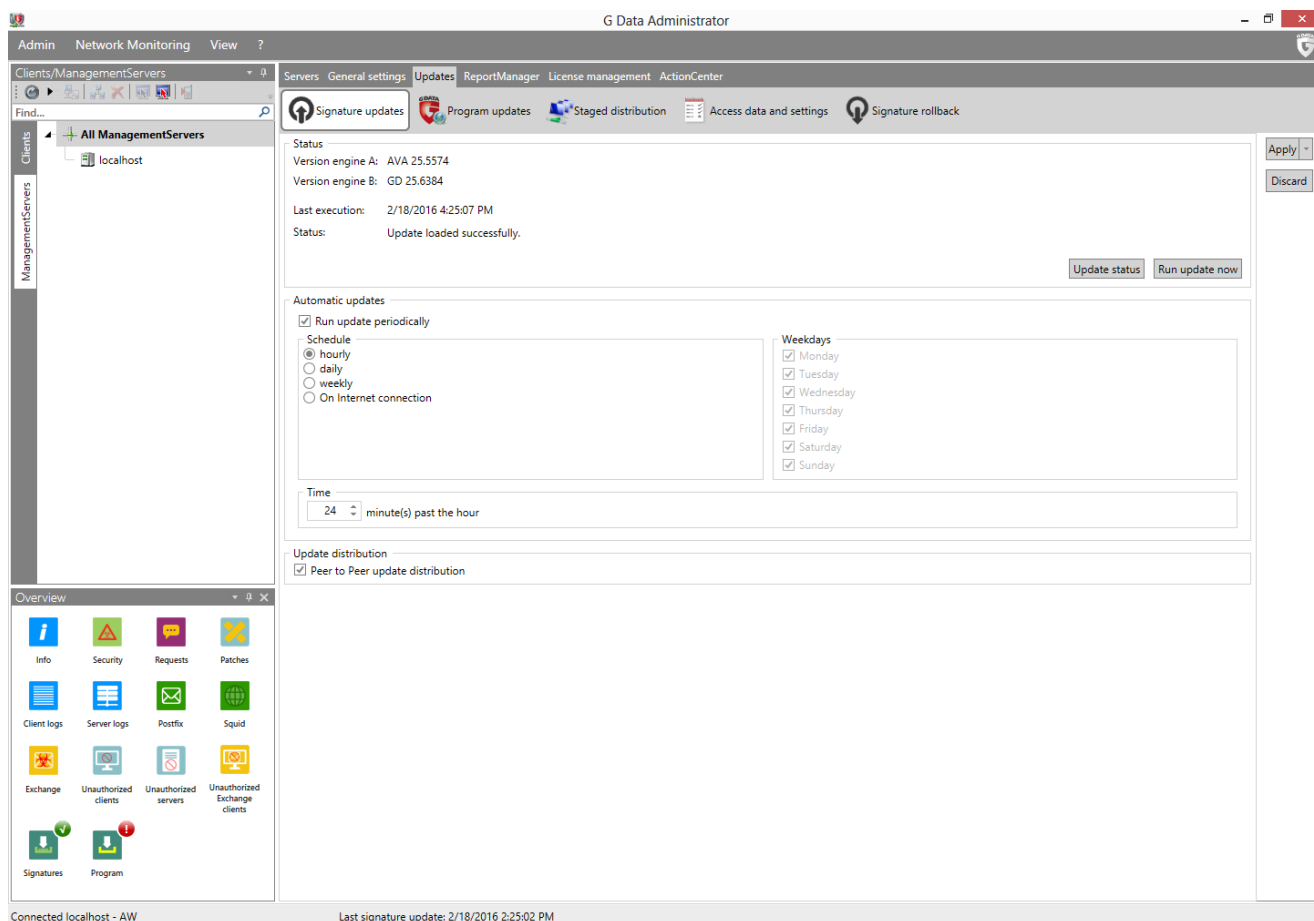
Under **Automatic updates**, the virus signature update can be scheduled. To do this, check the box next to **Run update periodically** and specify when and with what cycle the update is to be carried out. To enable automatic updating, your G DATA ManagementServer must be connected to the Internet and you must have entered the user name and password that you have received upon registration under **Updates** > **Access data and settings**. If the server connects to the Internet via a proxy server, your proxy credentials must also be entered there.

Updates can be distributed centrally (from the ManagementServer or subnet server to clients) or, if you activate **Peer to Peer update distribution**, decentralised (allowing already updated clients to distribute updates to other clients). Be sure to check the **port requirements** for this option.

4.4.3.2. Program updates

On the Program updates panel, you can configure the process of downloading program file updates from the G DATA update server to G DATA ManagementServer.

The following information and settings are available under **Program files (Client)**:

- **Current version**: The current version of the client program files on G DATA ManagementServer.
- **Last execution**: Timestamp for the last execution of the program file update process.
- **Status**: The status of the program file update process.
- **Update status**: Update the **Status** field.
- **Run update now**: Carry out an immediate update of the client program files on G DATA ManagementServer.
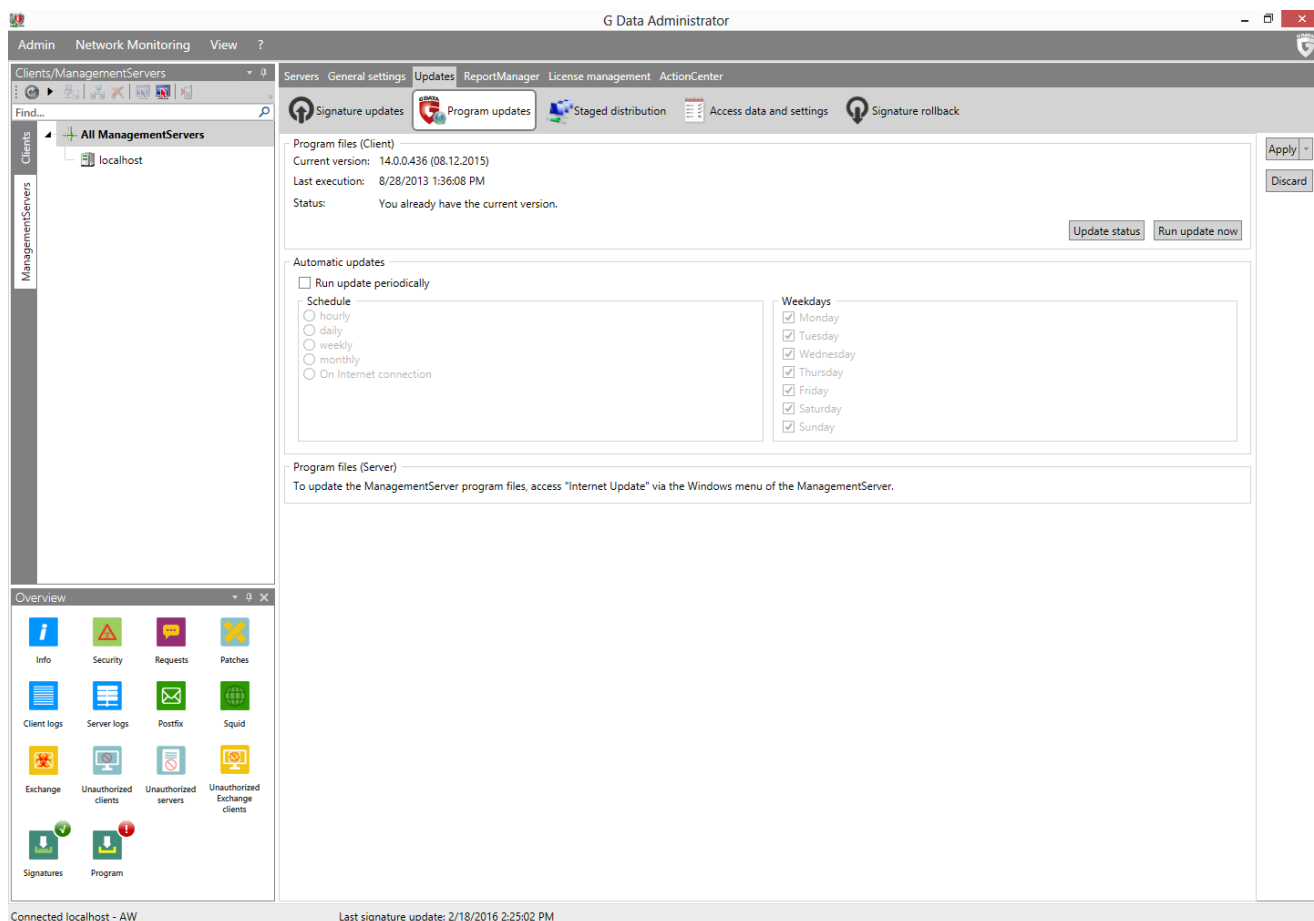
Under **Automatic updates**, the program file update can be scheduled. The settings are identical to those under **Signature updates**.

> G DATA ManagementServer itself can only be updated via the Start menu. 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.

4.4.3.3. Staged distribution

On the Staged distribution panel, you can set the distribution of client program file updates to be staged or to happen immediately. Staged distribution ensures that program file updates do not cause problems in the network environment and decreases the system load of simultaneous 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 updates. You can also choose the total number of groups and the delay between distribution among the different groups.
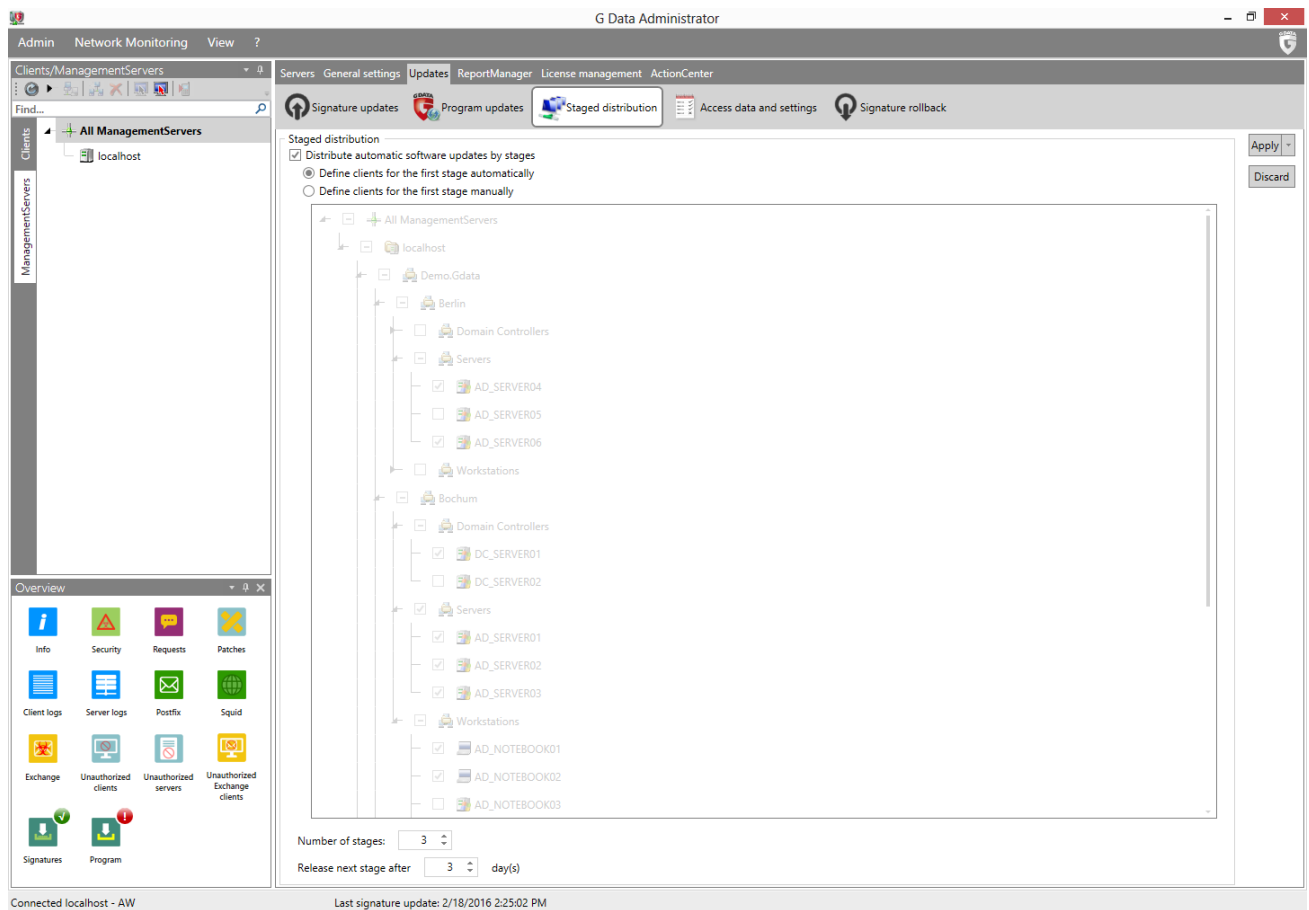
4.4.3.4. Access data and settings

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.
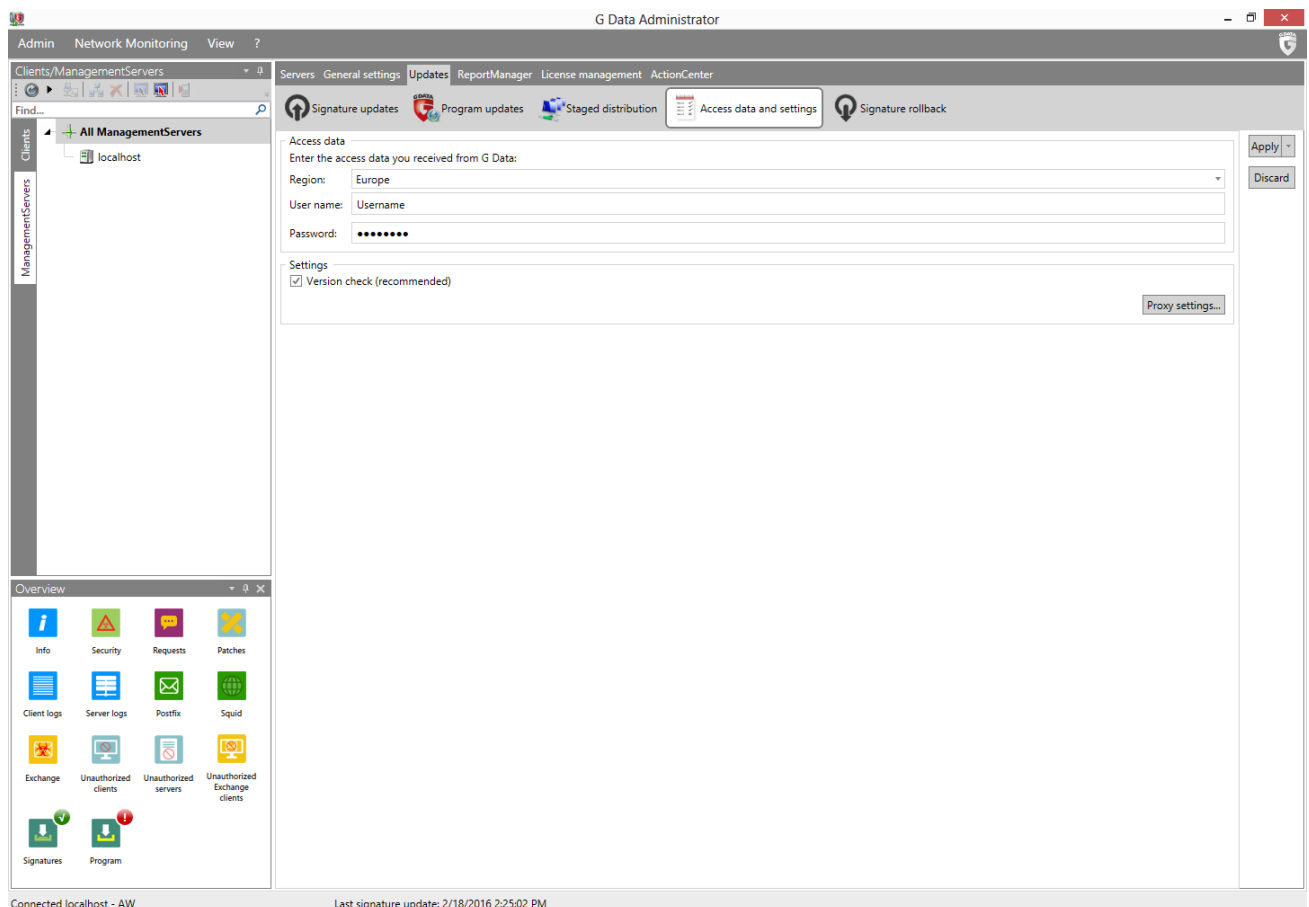
The **Version check** (enabled by default) should always be switched on because it improves update speed. If, however, problems arise with virus signature databases, switch off the version check. During the next update, the integrity of all virus signature database files will be checked and files will be redownloaded if necessary.

Proxy settings opens a window in which proxy server credentials can be entered. You should only enter these if an 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).

4.4.3.5. Signature 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. Under **Rollbacks** you can indicate how many of the 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.

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.

> 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.

4.4.4. 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.

The toolbar offers the following options:

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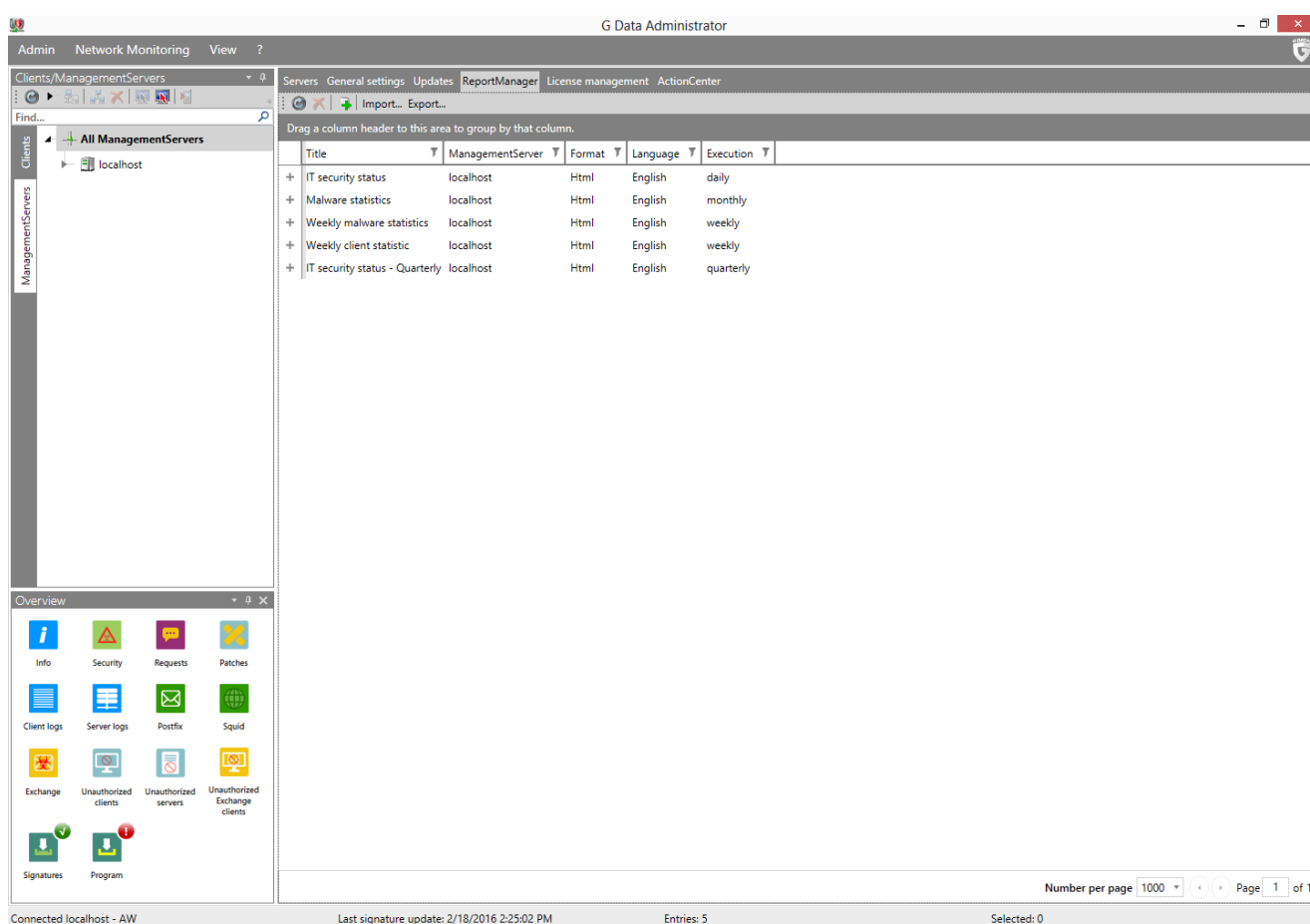
To backup report definitions, click **Export** to save them as a .dbdat file. Click **Import** to restore definitions. Right-click one or more report definitions to **Delete** them or click **Execute immediately** to run the reporting job immediately. Click **Properties** to edit a report definition.

4.4.4.1. 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 **General settings** > **Email** > **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 G DATA solution 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:

- **Limit**: For some modules, you can define a **Limit** to the amount of items to be included.
- **Client type**: You can optionally limit the type of clients that will be included in the report to either **Windows**, **Linux** or **Mac** clients.
- **Output format**: 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
- **Period covered**: Select an absolute or relative period of time that should be covered by the report.

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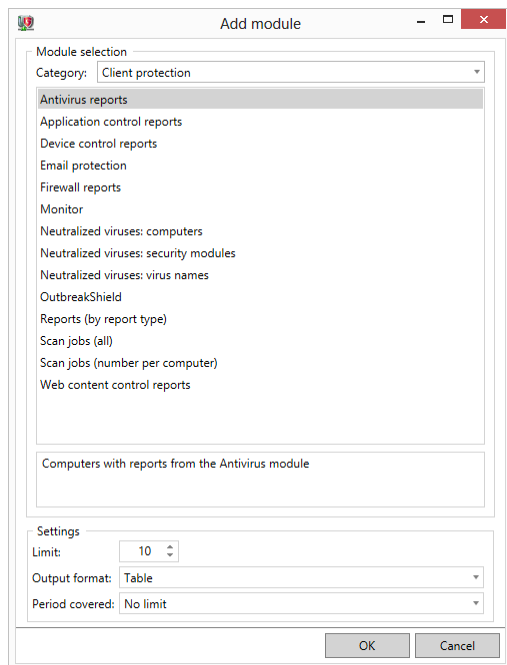
When a reporting job has been run, the resulting report will appear in the **ReportManager overview** and it will be sent to the defined recipients. Expand the report definition to see the full report history. Double click on an instance to open the associated report.

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.

4.4.5. License management

Using the License management panel you can have an overview of the G DATA software licenses that are currently in use. If you need additional licenses, you can get in contact with G DATA at any time by selecting a license and clicking **Extend license**.
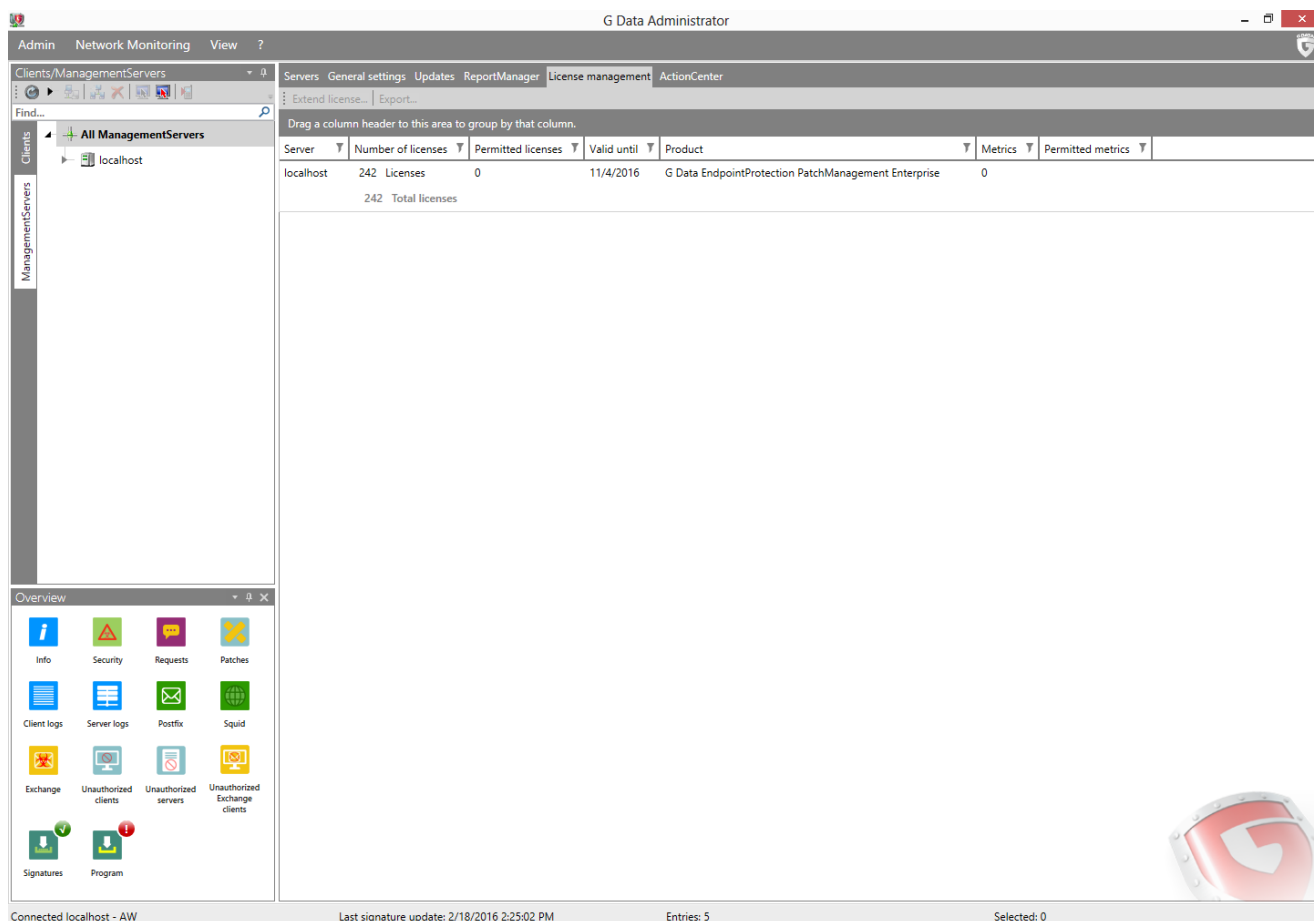
Using the button **Export** you can export the license information to a text file.

4.4.6. ActionCenter

G DATA Administrator connects to G DATA ActionCenter in order to manage iOS devices and to enable network monitoring. Create an account and enter the **User name** and **Password** here.

The use of G DATA ActionCenter requires a valid G DATA license. Make sure that you have entered your Internet Update **User name** and Internet Update **Password** under **Updates** > Access data and settings.

> The communication with G DATA ActionCenter depends on security features that are available in Windows Vista and newer. iOS Mobile Device Management and Network Monitoring are not available on G DATA ManagementServer and G DATA Administrator machines that are running Windows XP or Windows Server 2003.
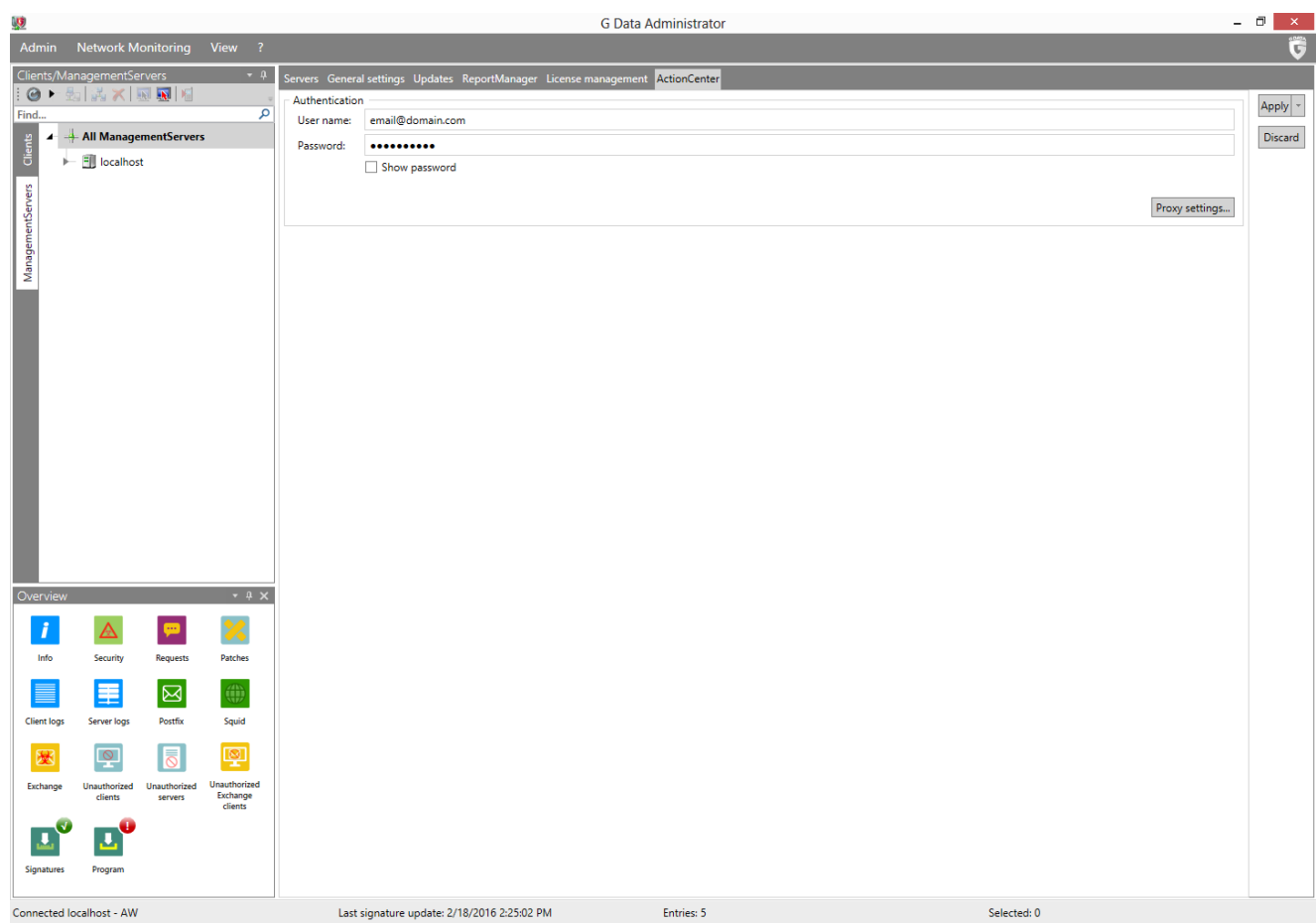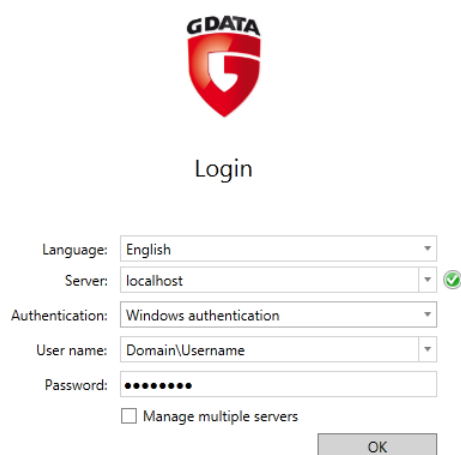
5. G DATA WebAdministrator

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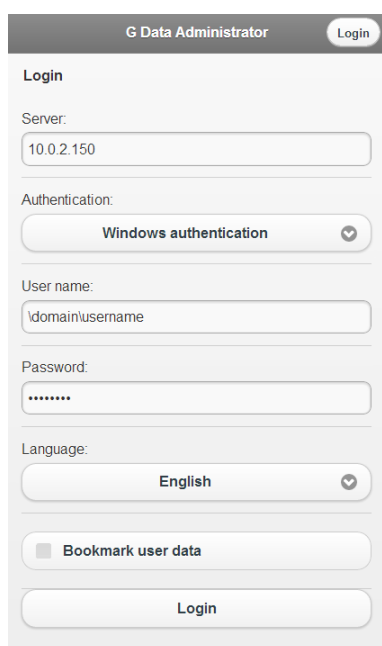
The functionality of WebAdministrator is identical to G DATA Administrator. Please refer to the **appropriate chapter** for an in-depth overview.

6. G DATA MobileAdministrator

G DATA MobileAdministrator is the mobile-friendly 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 MobileAdministrator 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 **G DATA WebAdministrator**. You will be prompted to enter **Language**, **Server**, **Authentication**, **User name** and **Password**. Choose **Windows authentication** to log in with your Windows (domain) credentials or **Integrated authentication** to use credentials that have been defined within the Administrator's **Manage users** window. 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**.
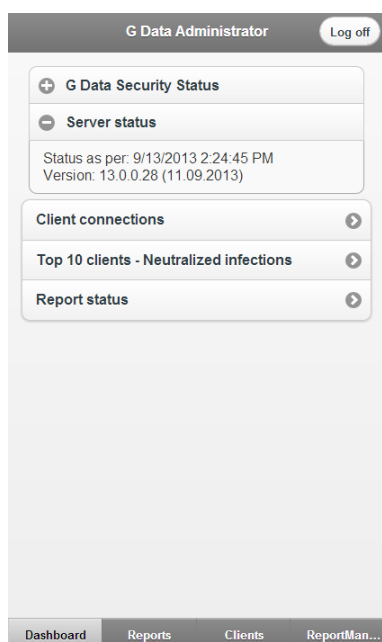
Statistics are available under **Client connections** and **Top 10 clients - Neutralized infections**. Tap **Report status** to check on infection, request and error reports.
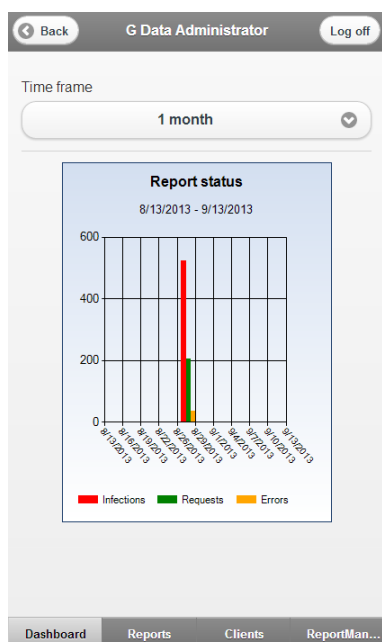
6.2.2. Reports

The Reports view presents virus, firewall and PolicyManager reports. It is a mobile-optimized representation of the same information that is available in the Security events 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.
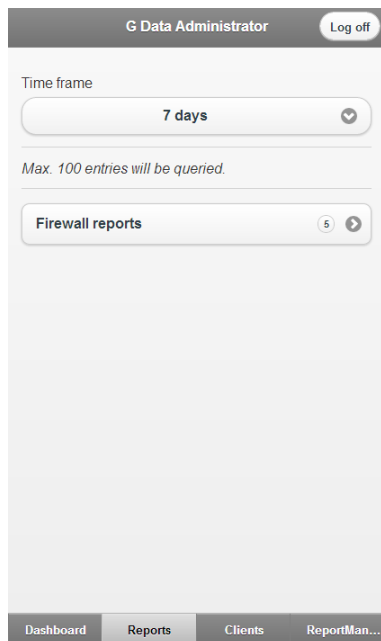
6.2.3. Clients

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.
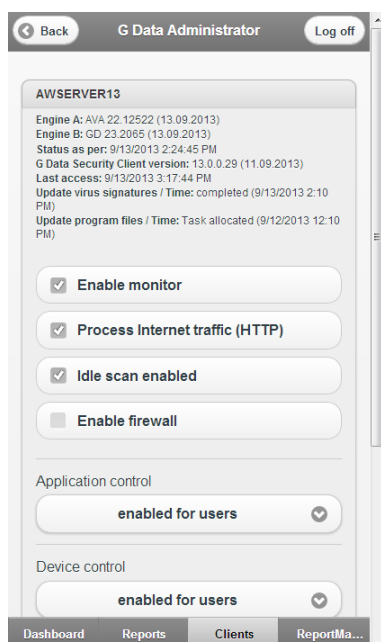
6.2.4. ReportManager

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 **Recipient groups** or enter **Additional recipients**. The job can be scheduled by selecting an **Interval** and defining time and date. Under **Selected module**, 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.
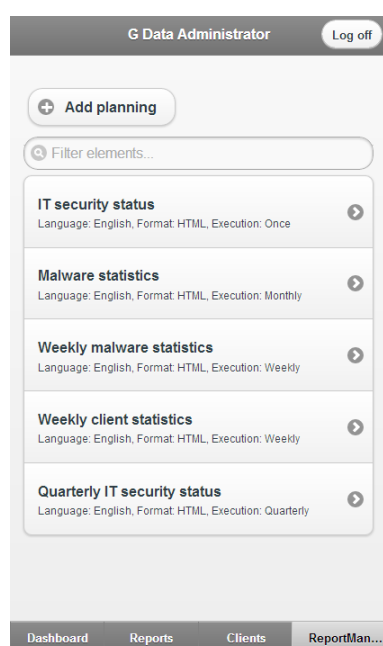
7. G DATA Security Client

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

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, click the G DATA Security Client icon to open a context menu which offers access to all Security Client functions.

7.1. 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.
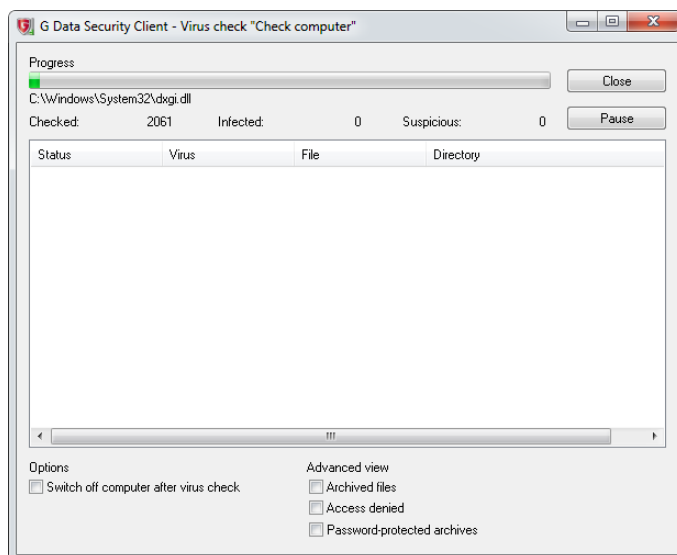
The user can check removable devices, CDs/DVDs, memory, the Autostart area, and individual files or directories. In this way, notebook users who only rarely connect their computers to the company network can prevent a virus attack in a targeted manner. Clients can use the **Options** window to configure 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**.

7.2. 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**.
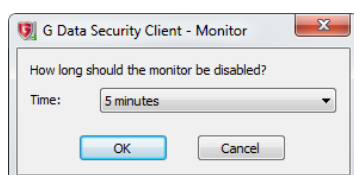
7.3. Options

Using the **Options** window, the user can configure security for the **Monitor**, **Email**, **Virus check** (local), **Web 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 window can be enabled or disabled in G DATA Administrator under **Client settings** > **General** > **Client functions**.

7.4. 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. More information about the quarantine folders can be found in the chapter **Default storage locations and paths**.

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**.

7.5. Updates/Patches

PatchManager is available as an **optional module**.

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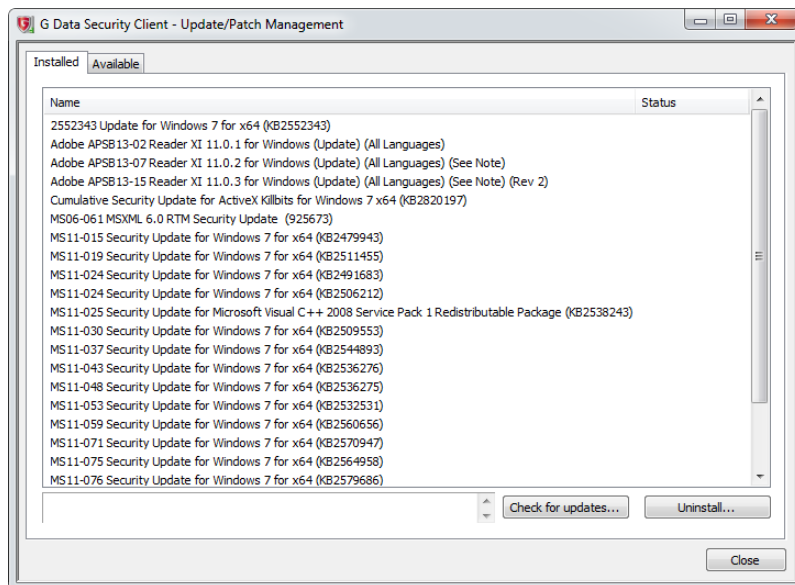
The **Installed** tab shows all patches and updates that have been installed on the system. Double click a patch to view an extended description. If a patch or update seems to be causing problems, users can select it and click **Uninstall** to ask the administrator to remove it. The **Status** will change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

7.6. 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 (see **Client settings** > **General** > **Updates**).

The **Internet update** system tray menu option can be enabled or disabled in G DATA Administrator under **Client settings** > **General** > **Client functions**.
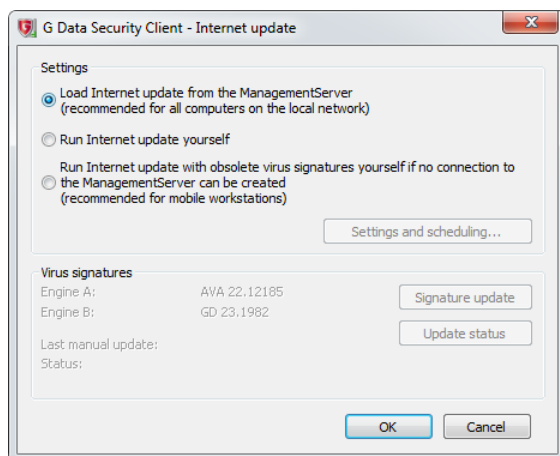
7.7. Disable firewall

The Firewall module is available as part of the Client Security Business, Endpoint Protection Business and Managed Endpoint Security **solutions**.

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 **Firewall** > **Overview** > **Run in internal network** by checking **Allow user to enable/disable the firewall**.

7.8. Firewall

The Firewall module is available as part of the Client Security Business, Endpoint Protection Business and Managed Endpoint Security **solutions**.

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** system tray menu option can be enabled or disabled in G DATA Administrator under **Firewall** > **Overview** > **Run outside internal network** by checking **Allow user to change the off-site configuration**.

7.8.1. Status

The Status module of the firewall shows information about the current status of the firewall. By double-clicking any of the entries, you can carry out actions directly or switch to the respective program area.

- **Security**: Enable or disable the firewall. This option is only available if it has been enabled in G DATA Administrator (**Firewall** > **Overview** > **Run in internal network** > **Allow user to enable/disable the firewall**).

- **Mode**: The firewall can be operated in automatic (autopilot) mode or in manual (rule sets) mode. Changing this option client-side is only possible if the client is being used outside the ManagementServer network and if it has been enabled in G DATA Administrator (**Firewall** > **Overview** > **Run outside internal network** > **Allow user to change the off-site configuration**).

- **Networks**: Open the **Networks** panel, which shows the networks that your computer is connected to as well as the rule sets that are used.

- **Prevented attacks**: When the firewall registers an attack on your computer, it is prevented and logged here.

- **Application radar**: Show which programs are currently being blocked by the firewall. If you want to allow one of the blocked applications to use the network, select it and then click the **Allow** button.
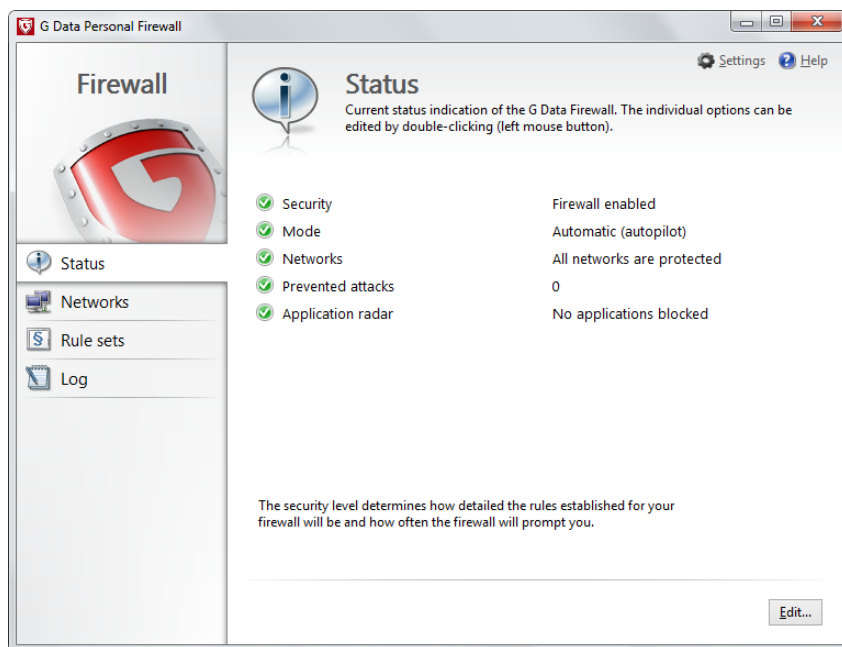
7.8.2. Networks

The Networks module lists all networks to which your computer is connected, as well as which rule set is protecting the respective network. Select a network and click **Edit** to view details and to configure the settings for this network. Network settings can only be edited if that has been specifically allowed (**Firewall** > **Overview** > **Run in internal network** > **Allow user to enable/disable the firewall**) or if the device is being used in off-site mode (**Firewall** > **Overview** > **Run outside internal network** > **Allow user to change the off-site configuration**).
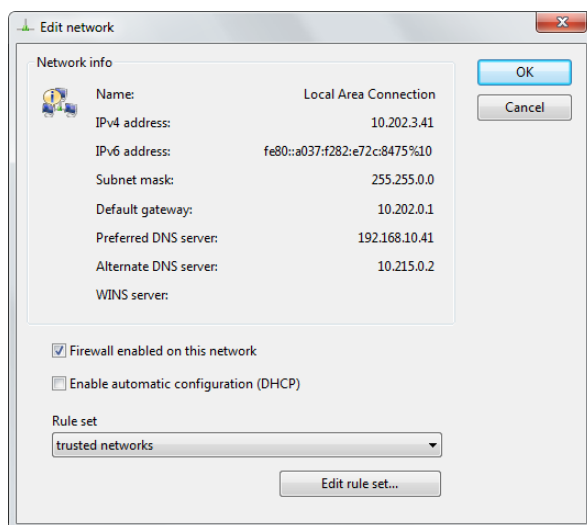
- **Network info**: Shows information about the network, including IP address, subnet mask, default gateway, DNS and WINS server.

- **Firewall enabled on this network**: Enable or disable firewall protection.

- **Internet connection sharing**: Allow Internet Connection Sharing.

- **Enable automatic configuration (DHCP)**: Allow DHCP configuration.

- **Rule set**: Choose any of the defined **Rule sets** to be applied to this connection. Click **Edit rule set** to open the **Rule Wizard**.

7.8.3. Rule sets

In the Rule sets module you can create and edit rule sets (groups of firewall rules that can be applied to networks).
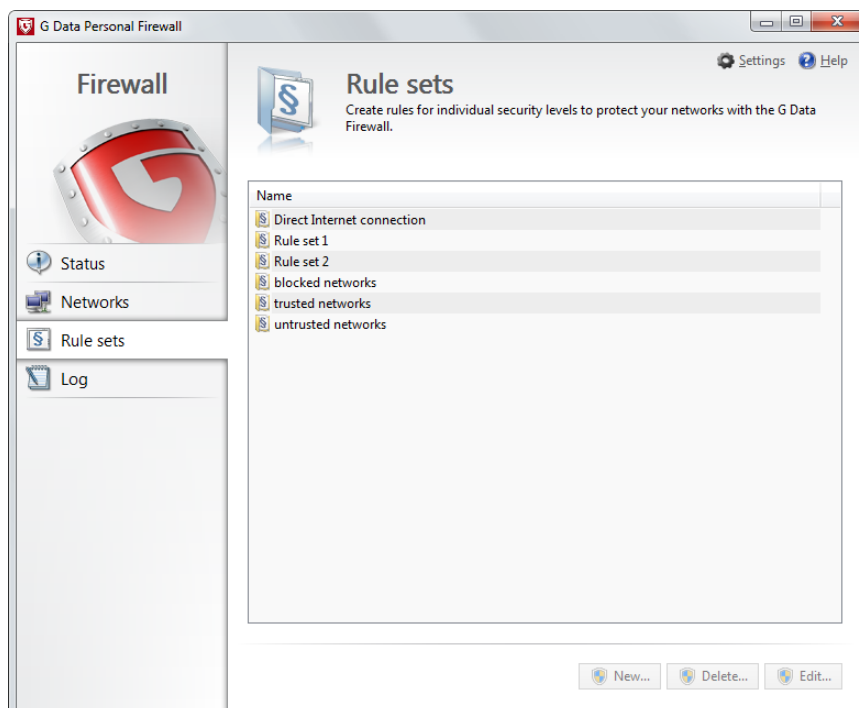
- **New**: Create a new rule set. In the following dialog, enter a **Rule set name** and decide if the rule set should be pre-populated with rules from the default rule sets for untrusted, trusted or blocked networks.

- **Delete**: Delete the selected rule set. The default rule sets cannot be deleted.

- **Edit**: Edit the selected rule set using the **Rule Wizard**.

The Rule sets module contains default rule sets for the following network types:

- **Direct Internet connection**: This covers rules that involve direct Internet access.

- **Untrusted networks**: This generally covers open networks with Internet access.

- **Trusted networks**: Home and company networks are generally trusted.

- **Blocked networks**: This rule set can be used if access to a specific network should be blocked.

7.8.3.1. Rule Wizard

The Rule Wizard allows you to define new rules for the selected rule set or to modify existing rules. The Rule Wizard is especially suitable for users unfamiliar with firewall technology. For a granular control over individual rules, use the **Advanced Rule Set Editor**.

The Rule wizard offers various rules. All of them can be used to quickly allow or deny a specific type of traffic. For most rules, a specific **Direction** can be defined, which governs whether the program is to be blocked for inbound connections, outbound connections or both.

- **Share or block applications**: Select a specific application on the hard disk to explicitly permit or deny it access to the network governed by the rule set.

- **Share or block network services**: Blocking one or more ports is a quick way of eliminating vulnerabilities that could be used for attacks by hackers. The wizard provides the option of blocking ports completely or for a particular application only.

- **File/printer sharing**: Allow or block file and printer sharing.

- **Share or block domain services**: Allow or block network domain services.

- **Shared use of the Internet connection**: Allow or block Internet connection sharing (ICS).

- **Share or block VPN services**: Allow or block Virtual Private Network (VPN) services.

- **Advanced Rule Set Editor (expert mode)**: Open the **Advanced Rule Set Editor**.
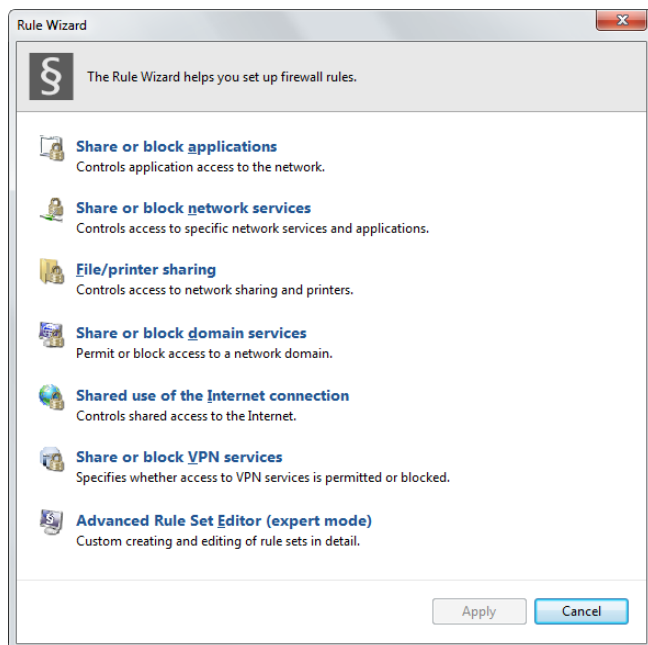
7.8.3.2. Advanced Rule Set Editor

The Advanced Rule Set Editor allows for the creation of highly specific rules. It can be used to create all of the rules that are also available through the Rule Wizard, but also supports custom settings.
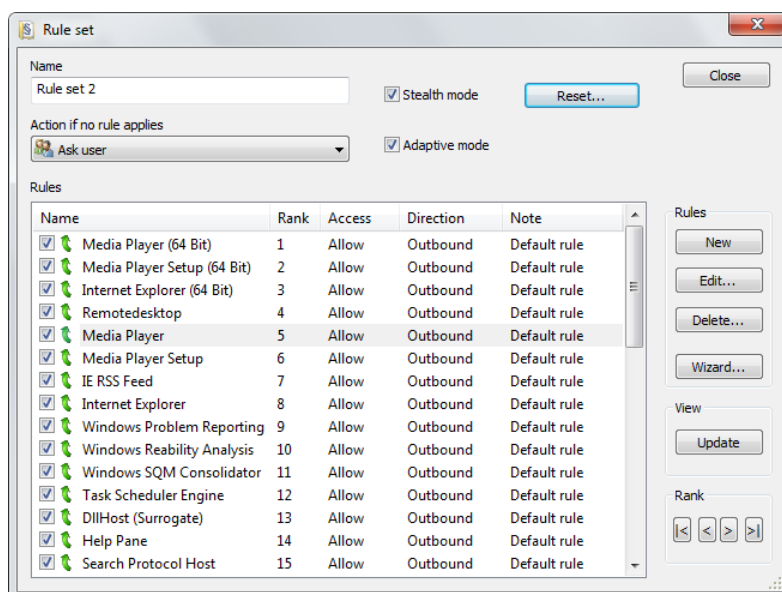
The Advanced Rule Set Editor window resembles the **Rule sets** pane of G DATA Administrator's

Firewall module. It can be used to create, edit, delete, and rank rules within the rule set. In addition to the options available in G DATA Administrator, the Advanced Rule Set Editor offers the following options:

- **Action if no rule applies**: Specify what happens when no existing rule applies to a filtered communication type: **Allow**, **Deny** or **Ask user**.

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

- **Reset**: Delete all rule sets modifications as well as all auto-learned rules.

By double-clicking a rule or clicking the **Edit** button, individual rules can be edited. The individual rule editor corresponds to the **Edit rule** window in G DATA Administrator.

7.8.4. Log

The Log module shows a detailed overview of all incoming and outgoing connections. It can be used to check the connection protocol, initiating application, direction, local port, remote host, remote port and reason for the decision about allowing or blocking the connection.
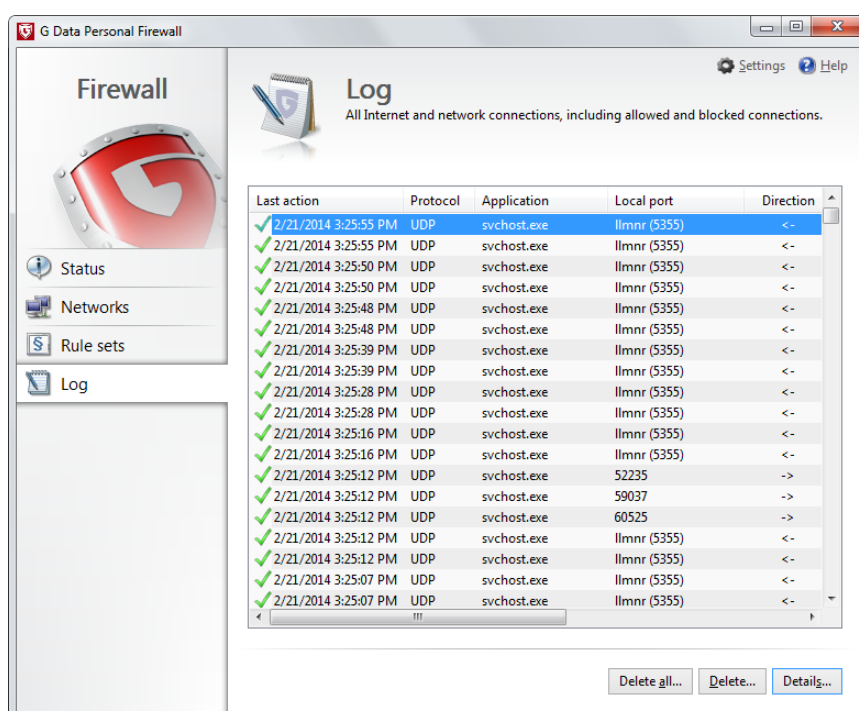
Click **Delete** to delete the selected log entry or **Delete all** to clear the log file completely. The **Details** button shows additional information about the selected log entry.

Right-click any log entry to access context-sensitive options. In addition to the **Details** view, these options include creating a new rule based on the log entry, editing the rule that led to the connection being blocked or allowed, and setting a filter view for the Log module.

7.8.5. Settings

The Settings window can be used if the appropriate permissions have been enabled in G DATA Administrator (**Firewall** > **Overview** > **Run in internal network** > **Allow user to enable/disable the**

firewall and **Firewall** > **Overview** > **Run outside internal network** > **Allow user to change the off-site configuration**).

- **Security**: Enable or disable the firewall.
- **Mode**: The firewall can be operated in automatic (autopilot) mode or in manual (rule sets) mode.

8. G DATA Security Client for Linux

G DATA Security Client for Linux runs as a background service and provides virus scan capabilities. For Linux servers, additional modules for Samba, Sendmail/Postfix and Squid are available (see **Installing G DATA Security Client for Linux**).

G DATA Security Client for Linux consists of a **graphical user interface** component and a **command line application**.

8.1. Graphical user interface

A shortcut to the graphical user interface of G DATA Security Client for Linux will be placed in the Applications menu or a similar place, depending on the Linux distribution. Alternatively, start the interface by running */opt/gdata/bin/gdavclient-qt.*

> After starting the interface, click the G DATA Security Client for Linux icon to open its interface. Which options are available can be configured using the **Client settings** module of G DATA Administrator.

Click the tray icon to open a context menu which offers access to the following settings:

- **Virus scan**
- **Quarantine**
- **Update**
- **Help**
- **Open G DATA Security Client**: Opens G DATA Security Client for Linux and displays the **Status** module.
- **About G DATA Security Client**

All modules can be protected against changes to settings (see **Client settings** > **General** > **Client functions**). If password protection has been enabled, click the lock in the left bottom corner of the window and enter the password to be able to change settings.

8.1.1. Status

The Status module offers an at-a-glance overview of the current protection status of the client. The status icons can be used to assess whether there is an immediate risk for the client or if the client is completely secure.

- **Latest scan**: The time and date of the last **Virus scan**. Use the **Scan computer now** button to immediately start a complete virus scan.
- **Latest update**: The time and date of the last **Update**. Use the **Update now** button to immediately start a virus signature update.

8.1.2. Virus scan

The Virus scan can be used to scan the complete computer or specific files or folders for malware. When a virus is found, the client will automatically take the action defined under **Settings**. ManagementServer will be notified and a report will be added to the **Security events** module of G DATA Administrator.

Select one of the following three options and click **Start virus scan**:

- **Scan complete computer**: Scan all files and folders on the computer.
- **Scan boot sector**: Scan the boot sector.
- **Scan files and folders**: Scan specific files and folders. The scope can be defined under **Scan scope**.

The following settings can be configured:

- **Reaction to infected files**: Define what should happen when the virus scan detects an infected file:
  - **Log only** (see **Client settings** > **Monitor** > Settings)
  - **Disinfect** (see **Client settings** > **Monitor** > Settings)
  - **Delete** (see **Client settings** > **Monitor** > Settings)
  - **Quarantine** (see **Client settings** > **Monitor** > Settings)
  - **Ask user**: Show a notification to the end user and ask which action should be taken.
- **If disinfection fails**: If the option **Disinfect** has been selected but the file cannot be disinfected, an alternate action will be carried out.
- **Reaction to infected archives**: Define what should happen when the virus scan detects an infected archive.
- **File types** (see **Tasks** > **Scan jobs** > Scanner)

Under **Advanced**, the following advanced settings can be configured:

- **Heuristics** (see **Client settings** > **Monitor** > Settings)
- **Check boot sector** (see **Client settings** > **Monitor** > Settings)
- **Check archives** (see **Client settings** > **Monitor** > Settings)
- **Archive size limit** (see **Client settings** > **Monitor** > Settings)
- **File size limit**: Define a maximum size. Files that are larger will not be scanned.

Use the file and folder list under **Exceptions** to exclude specific items from the scan.

The Virus scan module can be enabled or disabled in G DATA Administrator under **Client settings** > **General** > Client functions.

8.1.3. Update

The Update module makes sure that G DATA Security Client for Linux has the latest virus signatures in order to offer optimal protection.

The date and time of the last signature update are displayed under **Last update**. Signature version information for both virus engines is displayed under **Engine A** and **Engine B**. Click **Update virus signatures** to start a virus signature update right away.

The virus signature update settings can be configured under **Settings**:

- **Virus signature update source**: Configure whether the client should download virus signatures from ManagementServer or directly from the G DATA update servers (see **Client settings** > **General** > Updates).

- **Schedule**: Define a signature update schedule (**Manually**, **Hourly** or **Daily**).
- **Proxy server**: Enter a proxy server that should be used to connect to the G DATA update servers.
- **Access data**: Enter the access data that should be used to authenticate with the G DATA update servers.

The **Schedule**, **Proxy server** and **Access data settings** are only used if the **Virus signature update source** setting has not been set to **Download virus signature updates from ManagementServer**. See **Client settings** > **General** > **Updates** for more information.

The Update module can be enabled or disabled in G DATA Administrator under **Client settings** > **General** > **Client functions** (**Allow the user to download signature updates**).

8.1.4. Quarantine

The Quarantine module displays items that have been moved to the quarantine by the **Virus scan**.

Per item, the following properties are displayed:

- **File name**: The name and path of the infected item.
- **Virus name**: The name of the virus that infected the item.
- **File size**: The file size of the item.

Select one or more items and click one of the following buttons:

- **Disinfect and move back**: Remove the virus from the item and move the item back to its original location.
- **Move back**: Move the item back to its original location. Warning: if the item is not disinfected first, it might infect the system!
- **Delete**: Delete the item from the Quarantine.

The Quarantine module can be enabled or disabled in G DATA Administrator under **Client settings** > **General** > **Client functions**.

8.1.5. About G DATA Security Client

The About window displays status information about G DATA Security Client for Linux and can only be opened through the tray icon. It displays the following information:

- **Version**: The currently installed client version.
- **ManagementServer**: The current state of the connection to ManagementServer.
- **Security software status**: The current status of the client background services.

8.2. Command-line interface

As an alternative to the graphical user interface, command-line tools are available to configure and run G DATA Security Client for Linux. **Gdavclient-cli** is the preferred way of initiating a command-line virus scan and updating the virus signatures. Alternatively, **gdavclientc** can configure and run scans, display version information, update the virus signatures and manage the scan server daemon service. Both applications must be run as root to ensure full access to the file system.

8.2.1. gdavclient-cli

By default, gdavclient-cli is located in the folder /usr/bin. The syntax for gdavclient-cli looks as follows: *gdavclient-cli [<options>] <files/paths>*. The following options can be used:

- **--status**: Displays status for the gdavclientd and gdavserver daemons.
- **--version**: Displays version information.
- **--mmsconnection**: Displays information about the connection to G DATA ManagementServer.
- **--lastscan**: Displays the latest scan log.
- **--lastupdate**: Displays information about the latest virus signature update.
- **--update**: Updates the virus signatures.
- **--sysinfo**: Creates a file called gdatahwinfo-<Date>.tar.gz, which contains debug files such as logs and configuration files.

When a path or file(s) have been specified, gdavclient-cli initiates a virus scan.

8.2.2. gdavclientc

By default, gdavclientc is located in the folder /usr/bin. It is independent from G DATA ManagementServer and loads its configuration values from /etc/gdata/gdav.ini. The syntax for gdavclientc looks as follows: *gdavclientc [<options>] <command>*. The following commands can be used:

- **scan:<path>**: Initiate a scan of the file(s) at *<path>*. *<path>* can be an absolute or relative path to a file or a folder (which will be scanned recursively). Use of wildcards (*, ?) is allowed.
- **scanboot**: Perform a boot sector scan. All non-optical media that are listed under /proc/partitions will be scanned.
- **abort**: Abort the current scan.
- **start**: Start gdavserver.
- **stop**: Stop gdavserver.
- **restart**: Stop and restart gdavserver.
- **updateVDB<:engine>**: Initiate a virus signature update for EngineA or EngineB. After the update has completed, the scan server should be restarted using the *restart* command.
- **dump**: Show the current configuration.
- **set:<key>=<value>**: Set a specific option in the configuration of gdavserver, overwriting the existing option (which was read from /etc/gdata/gdav.ini). Options are only set temporarily and will be lost when stopping gdavserver.
- **get:<key>**: Show the current value of a specific option from the configuration of gdavserver.
- **reload**: Reload all values from /etc/gdata/gdav.ini.
- **engines**: List the names of all scan engines that are used.
- **baseinfo**: Show version information.
- **coreinfo**: Show virus engine version information.
- **pid**: Show the gdavserver PID.

If you use the **scan:** command to run a virus scan, the following options can be used:

- **-s**: In addition to the regular scan output, a summary of scan results will be displayed.
- **-x**: In addition to the regular scan output, a summary of scan results will be displayed (XML format).

9. G DATA Security Client for Mac

G DATA Security Client for Mac provides protection to Mac OS X clients. It runs scheduled virus scans and on-demand local scans and provides on-access protection through the Monitor module.

After the **installation** of the client software, a tray icon is available to the user. Which settings are available needs to be approved and defined using the **Client settings** module of G DATA Administrator.

Click the tray icon to open a context menu which offers access to the following settings:

- **Enable/disable monitor**
- **Virus scan**
- **Quarantine**
- **Update**
- **Help**
- **Open G DATA Security Client**: Opens G DATA Security Client for Mac and displays the **Status** module.
- **About G DATA Security Client**

All modules are protected against unintended changes to settings. Click the lock in the left bottom corner of the window to allow settings to be changed. If root permissions are required, the user will be prompted to enter user name and password.

9.1. Status

The Status module offers an at-a-glance overview of the current protection status of the client. The status icons can be used to assess whether there is an immediate risk for the client or if the client is completely secure.

- **Monitor**: The current status of the **Monitor**. Using the dropdown menu, it can be (temporarily) disabled.
- **Latest scan**: The time and date of the last **Virus scan**. Use the **Scan computer now** button to immediately start a complete virus scan.
- **Latest update**: The time and date of the last **Update**. Use the **Update now** button to immediately start a virus signature update.

9.2. Monitor

The monitor performs a background virus scan on all files that are accessed and takes action when it detects a virus.

The following settings can be configured:

- **Status**
  - **Enable monitor**: Enable the monitor (recommended).
  - **Disable monitor**: Permanently disable monitor. Disabling the monitor forms a security risk.
  - **Disable monitor until the next reboot**: Disable the monitor. After the next reboot, the monitor will be automatically enabled.

- o **Disable monitor for…minutes**: Disable the monitor for a specific number of minutes. The monitor will be automatically enabled afterward.
- **Reaction to infected files**: Define what should happen when the Monitor detects an infected file:
  - o **Log only** (see **Client settings** > **Monitor** > Settings)
  - o **Disinfect** (see **Client settings** > **Monitor** > Settings)
  - o **Delete** (see **Client settings** > **Monitor** > Settings)
  - o **Quarantine** (see **Client settings** > **Monitor** > Settings)
  - o **Ask user**: Show a notification to the end user and ask which action should be taken.
- **If disinfection fails**: If the option **Disinfect** has been selected but the file cannot be disinfected, an alternate action will be carried out.
- **Reaction to infected archives**: Define what should happen when the Monitor detects an infected archive.
- **File types** (see **Tasks** > **Scan jobs** > Scanner)

Under **Advanced**, the following advanced settings can be configured:

- **Heuristics** (see **Client settings** > **Monitor** > Settings)
- **Check boot sector** (see **Client settings** > **Monitor** > Settings)
- **Check archives** (see **Client settings** > **Monitor** > Settings)
- **Archive size limit** (see **Client settings** > **Monitor** > Settings)
- **File size limit**: Define a maximum size. Files that are larger will not be scanned.

Use the file and folder list under **Exceptions** to exclude specific items from the scan.

The Monitor module can be enabled or disabled in G DATA Administrator under **Client settings** > **General** > Client functions.

9.3. Virus scan

The Virus scan can be used to scan the complete computer or specific files or folders for malware. When a virus is found, the client will automatically take the action defined under **Settings**. ManagementServer will be notified and a report will be added to the Security events module of G DATA Administrator.

Select one of the following three options and click **Start virus scan**:

- **Scan complete computer**: Scan all files and folders on the computer.
- **Scan boot sector**: Scan the boot sector.
- **Scan files and folders**: Scan specific files and folders. The scope can be defined under **Scan scope**.

Under **Settings**, the virus scan settings and exceptions can be configured (see Monitor).

The Virus scan module can be enabled or disabled in G DATA Administrator under **Client settings** > **General** > Client functions.

9.4. Update

The Update module makes sure that G DATA Security Client for Mac has the latest virus signatures in order to offer optimal protection.

The date and time of the last signature update are displayed under **Last update**. Signature version information for both virus engines is displayed under **Engine A** and **Engine B**. Click **Update virus signatures** to start a virus signature update right away.

The virus signature update settings can be configured under **Settings**:

- **Virus signature update source**: Configure whether the client should download virus signatures from ManagementServer or directly from the G DATA update servers (see **Client settings** > **General** > **Updates**).
- **Schedule**: Define a signature update schedule (**Manually**, **Hourly** or **Daily**).
- **Proxy server**: Enter a proxy server that should be used to connect to the G DATA update servers.
- **Access data**: Enter the access data that should be used to authenticate with the G DATA update servers.

The **Schedule**, **Proxy server** and **Access data settings** are only used if the **Virus signature update source** setting has not been set to **Download virus signature updates from ManagementServer**. See **Client settings** > **General** > **Updates** for more information.

The Update module can be enabled or disabled in G DATA Administrator under **Client settings** > **General** > **Client functions** (**Allow the user to download signature updates**).

9.5. Quarantine

The Quarantine module displays items that have been moved to the quarantine by the **Monitor** or by a **Virus scan**.

Per item, the following properties are displayed:

- **File name**: The name and path of the infected item.
- **Virus name**: The name of the virus that infected the item.
- **File size**: The file size of the item.

Select one or more items and click one of the following buttons:

- **Disinfect and move back**: Remove the virus from the item and move the item back to its original location.
- **Move back**: Move the item back to its original location. Warning: if the item is not disinfected first, it might infect the system!
- **Delete**: Delete the item from the Quarantine.

The Quarantine module can be enabled or disabled in G DATA Administrator under **Client settings** > **General** > **Client functions**.

9.6. About G DATA Security Client

The About window displays status information about G DATA Security Client for Mac:

- **Version**: The currently installed client version.

- **ManagementServer**: The name of the ManagementServer to which the client connects.

- **Security software status**: The current status of the client background services.

10. G DATA ActionCenter

G DATA ActionCenter offers cloud-enabled G DATA services. Its functionality has been divided into modules. After **creating an account** and logging in to the web interface at **https://ac.gdata.de**, you can choose a module in the main screen under **Modules** or through the **Menu** in the top right corner:

- **Mobile devices**: Mobile device management for G DATA retail solutions.
- **Network Monitoring**: Monitor network infrastructure in order to prevent and provide quick response to outages.

The following shortcuts are listed under **Settings**:

- **Permissions**: Manage permissions for other ActionCenter accounts, such as read-only permissions for **Network monitoring**.
- **Email groups**: Configure email groups to enable reports and notifications, such as the alerts functionality of **Network monitoring**.

ActionCenter also enables iOS Mobile Device Management by providing communication between iOS devices and G DATA ManagementServer. The configuration of iOS Mobile Device Management is carried out through the **iOS Mobile Device Management** node in the **Clients** window of G DATA Administrator.

10.1. Creating and linking an account

At the login page of ActionCenter, click **Register** to open the registration page. After entering and confirming an **Email address**, entering a **Password** and agreeing to the terms and conditions, click **Register** to submit your data. An email containing a confirmation link will be sent to the email address.

After confirming the account by clicking the confirmation link, the user name and password should be configured in G DATA Administrator in the **ActionCenter** module in order to establish the link between G DATA ManagementServer and G DATA ActionCenter.

10.2. Modules

The functionality of G DATA ActionCenter has been divided into various modules. For business solutions, ActionCenter offers the Network Monitoring module.

10.2.1. Network monitoring

Network monitoring is available as an **optional module**.

Using network monitoring, administrators can keep an eye on the status of their network infrastructure. By defining **metrics**, a wide range of statistical information can be collected from clients and viewed through the Dashboard.

10.2.1.1. Dashboard

The Dashboard shows up-to-date statistics for all **metrics**, as well as an overview of all **servers** and **devices** that can be managed. When a metric is favorited, a summary widget is added to the Dashboard containing the associated device name, latest value and a trend diagram.
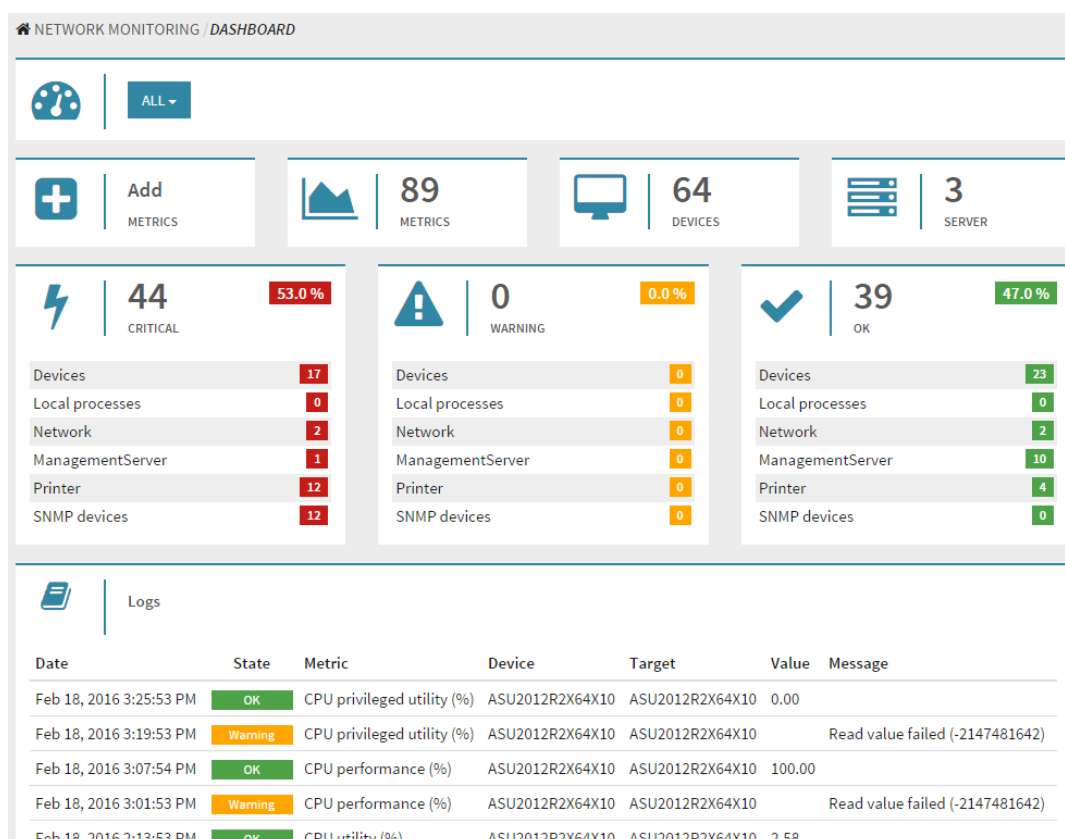
At the center of the Dashboard, status information is displayed. Under **OK**, all metrics that are not reporting any threshold violations are listed. When a metric reports a value above or below a previously defined threshold, its status is changed to **Warning**. After two more threshold violations, the status is changed to **Critical**. Per status, metrics are displayed by category. This allows for a granular overview of which device category is currently affected.

The **Logs** section displays log entries for all metrics. Log entries are added when a metric reports its first value, when it reports an error and when it changes its state (for example from **OK** to **Critical**). Clicking a log entry opens the associated **Metric** page.

When managing multiple servers, the dropdown list at the top of the Dashboard can be used to create and select Dashboard views. Click **Create dashboard**, enter a **Name** for the Dashboard and assign one or more ManagementServers.

10.2.1.2. Metrics overview

A metric is created by assigning a **metric template** to one or more devices. Based on the parameters in the metric template, the metric will regularly report the specified statistics from the specified device(s). Click **Create metrics** to **create a new metric**.

The Metrics overview page lists all metrics. Clicking a metric opens the associated **Metric** page. The metrics list can be filtered by state or category. For each entry in the list, the following information is displayed:

- **ManagementServer**: The ManagementServer governing the device to which the metric template has been assigned.
- **Device**: The device to which the metric template has been assigned.
- **State**: The current status of the metric (**OK**, **Warning**, **Critical** or **Unknown**).
- **Metric**: The name of the metric template which was used to create the metric.
- **Category**: The category of the metric template which was used to create the metric.

- **Target**: The target device of the metric template which was used to create the metric.

Add metrics

Creating a metric involves assigning one or more **metric templates** to one or more devices. The Add metrics page offers a four-step process:

1. **Choose metric templates**. Select one or more templates. The templates are listed by category.

2. **Choose devices**. Select one or more devices. The devices are displayed in a folder structure, grouped by ManagementServer. At the top level of the folder structure, the ManagementServers themselves can be selected (in case a metric template from the **ManagementServer** category has been chosen in step 1).

3. **Verify chosen devices**. Make sure that all devices to which the chosen template(s) should be applied have been selected.

4. **Summary**. Click **Create metric** to create the corresponding metric(s) and return to the **Metrics overview**.

Metric

The Metric page displays the details of the selected metric. At the top of the page, its **Name**, **Device** and **ManagementServer** are displayed, as well as its current status. Using the **Favorite** option, the metric can be pinned to the **Dashboard**.
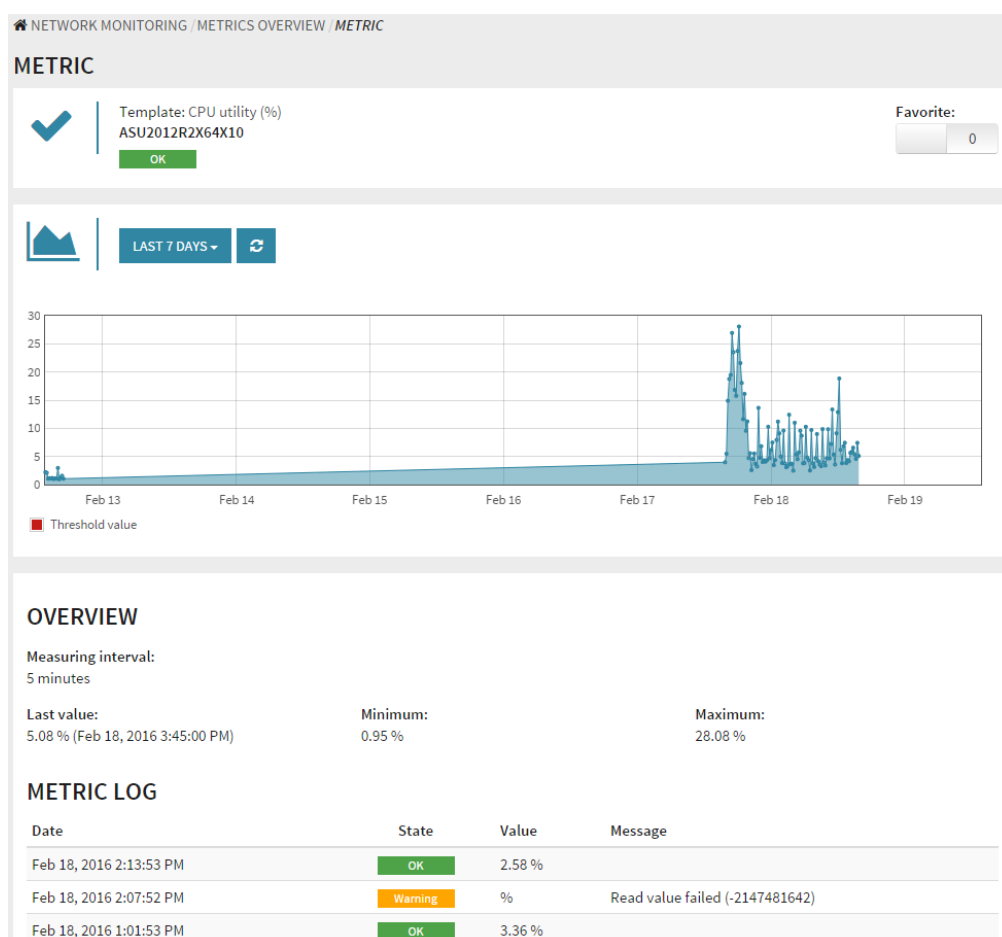
The diagram view can be customized to get an instant overview of trend data. The default setting shows the values for the last 6 hours. Using the dropdown menu, this range can be changed.

Under **Overview**, several parameters are displayed:

- **Measuring interval**: The interval with which the metric sends new values to ActionCenter.
- **Last value**: The most recent value including a timestamp.
- **Minimum**: The lowest value ever recorded.
- **Maximum**: The highest value ever recorded.
- **Threshold** (only displayed if a threshold has been set): The current threshold value.
- **Over threshold** (only displayed if a threshold has been set): The percentage of recorded values that was higher than the threshold value.
- **Under threshold** (only displayed if a threshold has been set): The percentage of recorded values that was lower than the threshold value.

Under **Metric log**, all log entries for the metric are displayed. Log entries are added when a metric reports its first value, when it reports an error and when it changes its state (for example from **OK** to **Critical**).

Manage metric templates

A metric template contains the parameters for a specific network monitoring scenario. Templates can be assigned to one or more devices, creating **metrics**.

The Manage metric templates page lists all metric templates. For each entry in the list, the following information is displayed:

- **Name**: The name of the template.
- **Comment**: Information that helps distinguish templates.
- **Category**: The category of the template (**Devices**, **Local processes**, **Network**, **ManagementServer**, **Network printer** or **SNMP devices**).
- **Metric**: Defines the type of information that is being monitored, depending on which **Category** has been selected.
- **Used by**: The number of devices to which a **metric** using this template has been assigned.

Clicking a template in the list to open the **Edit template** page. Click **Create template** to create a new metric template.

Create template

To create a metric template, a number of required and optional parameters should be entered:

- **Category**: Select the template category (**Devices**, **Local processes**, **Network**, **ManagementServer**, **Printer** or **SNMP devices**).

- **Metric**: Select the type of information that should be monitored, depending on which **Category** has been selected.

- **Name**: The name of the template.

- **Comment**: Information that helps distinguish templates.

⌂ NETWORK MONITORING / METRIC TEMPLATES / *CREATE*

GENERAL SETTINGS

Category:

[DEVICES ▾]

Metric:

[COUNT OF WINDOWS SYSTEM EVENT LOGS ▾]

Target:
LOCALHOST

Name:

| Count of Windows system event logs |

Comment:

| Count of Windows system event logs |

[⤓ SAVE TEMPLATE]

OPTIONAL SETTINGS

Threshold value:

| Threshold value |

Measured value condition:

| Value has to be above threshold ▾ |

[⤓ SAVE TEMPLATE]

ALERTS SETTINGS

Enabled:

[___ 0]

[⤓ SAVE TEMPLATE]

Depending on the **Category** and **Metric**, one or more of the following settings will be displayed:

- **Target**: The target on which the selected information will be collected. This value cannot be changed and is set to localhost by default, meaning that the information will be collected on the device to which the metric template will be assigned.

- **Hostname**: The host name of the device on which the selected information will be monitored. This does not necessarily need to be the device to which the metric template will be assigned.

Multiple host names can be added; when the metric template is assigned to a device, multiple metrics will be created.

- **URL**: The URL for which the selected information will be monitored. Multiple URLs can be added; when the metric template is assigned to a device, multiple metrics will be created.
- **SQL Server Instance**: The SQL Server instance on which the selected information will be monitored. Click the magnifying glass to view a list of available SQL Server instances per ManagementServer.

Optional settings also depend on the selected **Category** and **Metric** and include one or more of the following:

- **Threshold value**: Set a threshold value.
- **Measured value condition**: Dictates how the threshold value is interpreted. The metric state will change from **OK** to **Warning** and then to **Critical** when the measured value is below or above the threshold.
- **CPU**: Enter the CPU for which the selected information will be monitored or enter _Total to monitor all CPUs.
- **Drive letter**: Enter the drive for which the selected information will be monitored or enter _Total to monitor all drives.
- **Process name**: Enter the process name for which the selected information will be monitored or enter _Total to monitor all processes.
- **Network adapter name**: Enter the network adapter for which the selected information will be monitored or enter *to monitor all network adapters.
- **SQL Server Database**: Enter the database for which the selected information will be monitored or enter _Total to monitor all databases.
- **Request timeout**: Enter the request timeout for Ping requests.
- **Expected HTTP status code**: When the HTTP request returns a different status code from the one defined here, it is treated as a threshold violation, changing the metric state.
- **SNMP Community**: Enter the SNMP community string that is required by the target device. The community string is set by the manufacturer of the device and can often be found in the device's documentation.

Under **Alerts settings**, email alerts can be configured:

- **Alert condition**: An alert will be sent when the metric state changes to **Critical** only or when it changes to either **Critical or Warning**.
- **Notify only selected email groups**: The alert will be sent to the selected email groups, which can be defined using the **Email groups** page.

Edit template

The Edit template page can be used to edit existing metric templates. All settings correspond to the ones that were set when the template was created. Some are displayed as read-only and cannot be changed:

- **Category**
- **Metric**
- **Used by**

- **Target**
- **Hostname**
- **URL**

All other settings can be freely edited. Click **Save template** to save the changes. Changes made to an existing template will be applied to all metrics that are based on the selected template.

10.2.1.3. Server overview

The Server overview displays all ManagementServers that have been linked to the ActionCenter account. Per server, the number of associated **devices**, **metrics** and printers is listed. The overview can be filtered by clicking any of the tags under **Filter**.

Clicking a server opens the **Server info** page, which allows access to the following information and settings:

- **Hostname**: The host name of the server.
- **Version**: The version number of ManagementServer.
- **Last access**: The timestamp of the last synchronization between this server and ActionCenter.
- **Metrics**: The number of metrics associated with this server.
- **Devices**: The number of devices associated with this server.

- **Printers**: The number of printers associated with this server.

- **Comment**: Information that helps distinguish servers.

- **API access**: Enabled by default. Disabling API access does not remove the server from ActionCenter but prevents it from reporting values.

- **Tags**: Add one or more tags that can be used to filter the Server overview list.
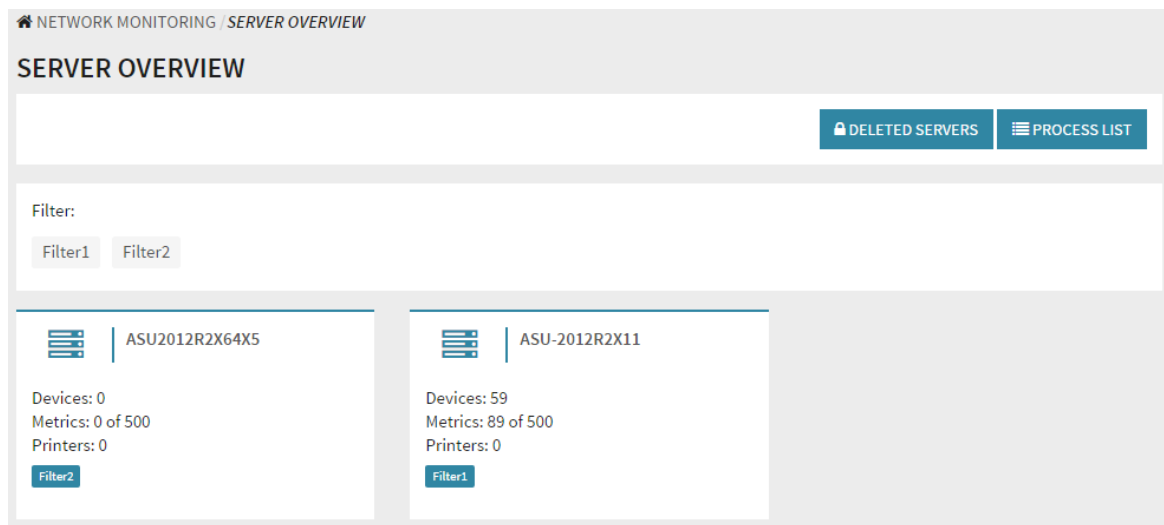
Click **Set permissions** to grant read-only permissions for this server to another ActionCenter account. Enter the account's email address under **Email** and click **Send invitation** to send an invitation email. After logging in to ActionCenter using the provided link and accepting the invitation, the recipient will have read-only access to all network monitoring functionality for this server. Permissions can be viewed and revoked using the **Permissions** page.

> If the email address is not yet associated with an ActionCenter account, the recipient will be prompted to create an account. Afterward, the invitation can be accepted.

Click **Delete server** to remove the server from ActionCenter. This will also remove all associated **devices**, **metrics** and logs.

10.2.1.4. Devices overview

The Devices overview lists all devices that are managed by the ManagementServers that have been linked to the ActionCenter account. The list can be filtered by clicking **Filter** and selecting the appropriate ManagementServer from the folder structure.

Each device is listed with its name and all associated metrics. Clicking a metric opens the associated Metric page.

10.3. Settings

The Settings area contains settings that can be used by other ActionCenter modules.

10.3.1. Permissions

The Permissions page can be used to manage permissions that have been granted under **Network monitoring** > Server overview. The ActionCenter accounts with permissions are listed under the headings of the respective ManagementServers. Click **Remove** to revoke the permissions for the selected account.

10.3.2. Email groups

Email groups bundle one or more email address and are used for reporting and notifications, such as the threshold alerts of the **Network monitoring** module. The Email groups page displays all email groups and their associated email addresses.

To create a new email group, click **Add email group**, enter a **Name**, select the intended **Language** and then click **Add**. To add an email address to a group, select the group and then, under **Edit group Group name**, enter an **Email address** and click **Add email to "Group name"**. This step can be repeated to add multiple email addresses to the same group.

11. G DATA MailSecurity MailGateway

G DATA MailSecurity is available as an **optional module**.

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.

12. G DATA MailSecurity Administrator

G DATA MailSecurity is available as an **optional module**.

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.
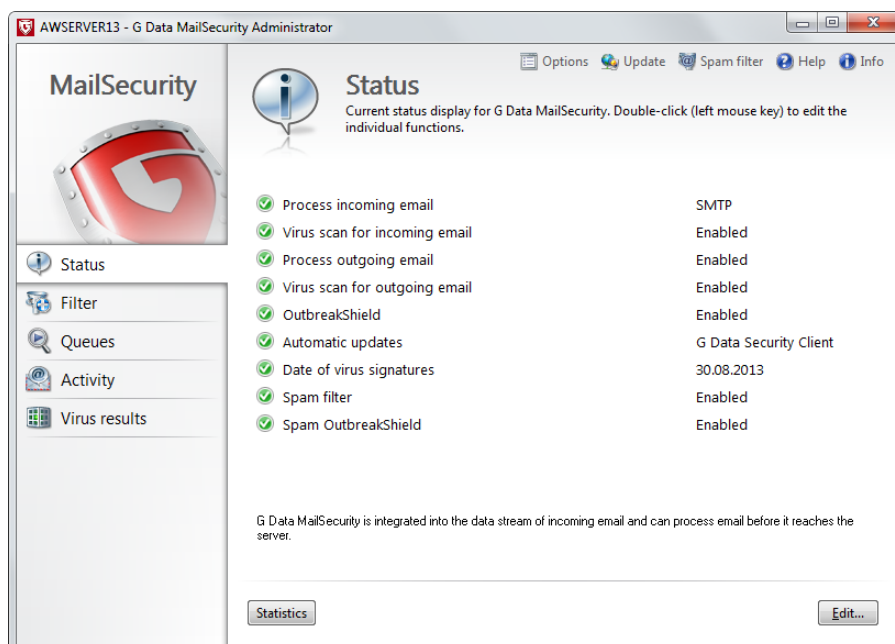
12.1. Starting G DATA MailSecurity Administrator

You can use Administrator to manage the mail gateway by clicking on the entry **G DATA MailSecurity** 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.

12.2. 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**: The Spam filter button provides a shortcut to the **Spam filter** settings of the **Filter** module.
- **Help**: Access the online help for the product.
- **Info**: Information about the program version.

12.2.1. 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.

12.2.1.1. Incoming (SMTP)

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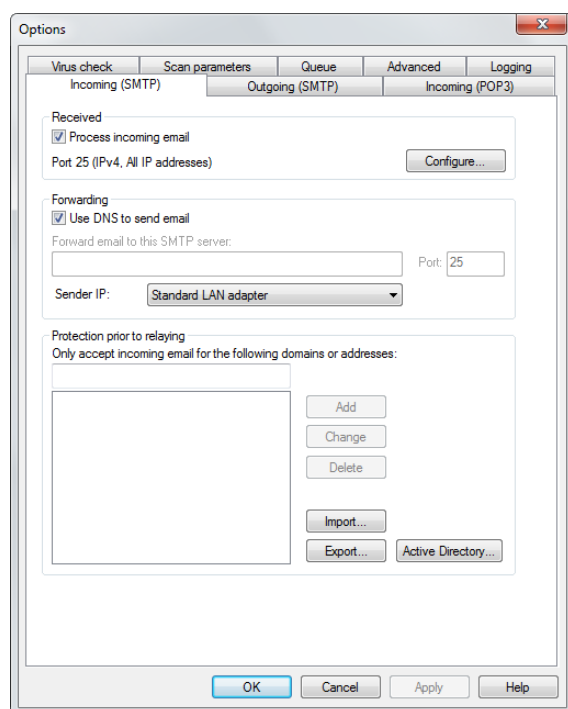
Received

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.

12.2.1.2. Outgoing (SMTP)

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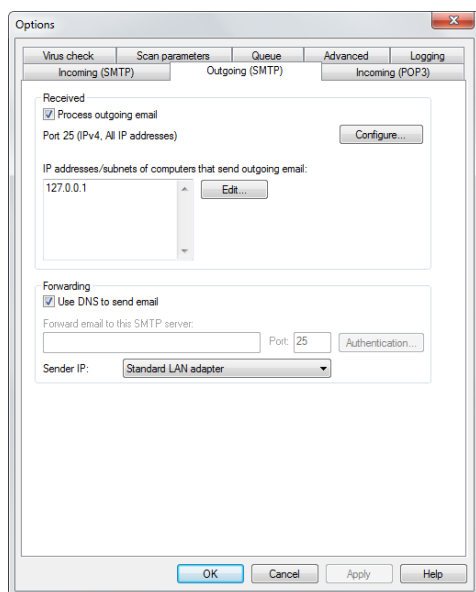
Received

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 outgoing 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.

12.2.1.3. Incoming (POP3)

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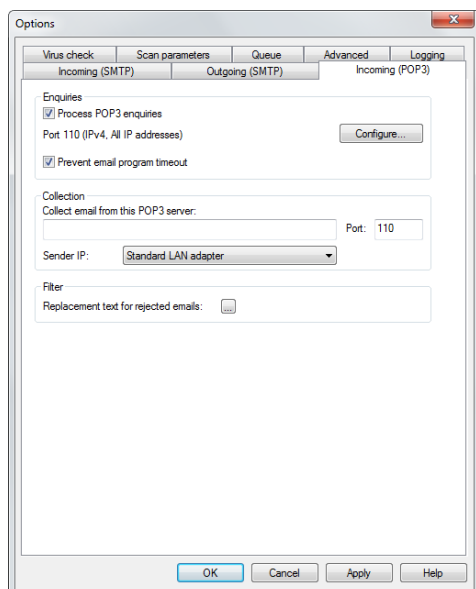
Enquiries

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

12.2.1.4. Virus check

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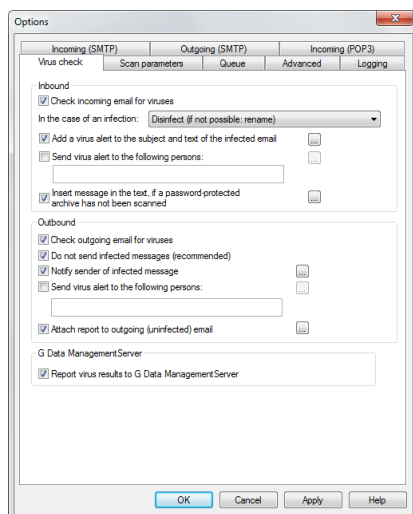
Inbound

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., by using G DATA Antivirus Business).

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.

12.2.1.5. 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.
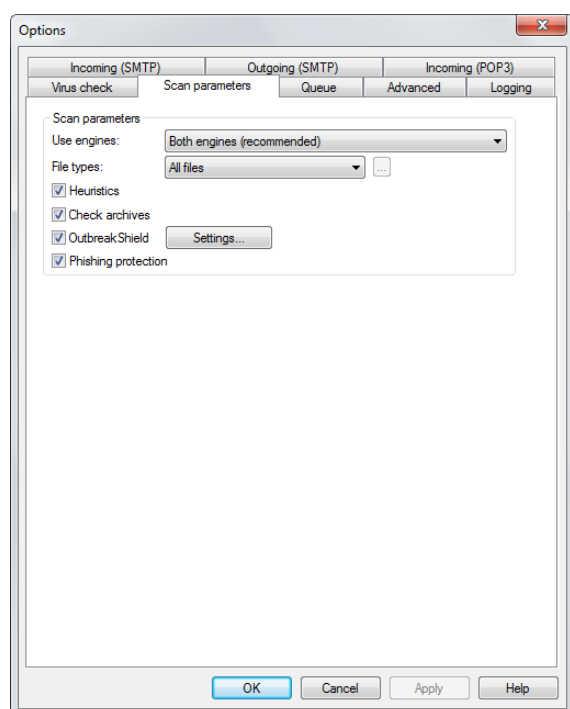
The following functions are available:

- **Use engines**: The G DATA software works with two independently operating virus scanning engines. Using both engines guarantees optimum virus detection. Using just one engine can 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 F 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** > **Inbound** 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.

12.2.1.6. 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.
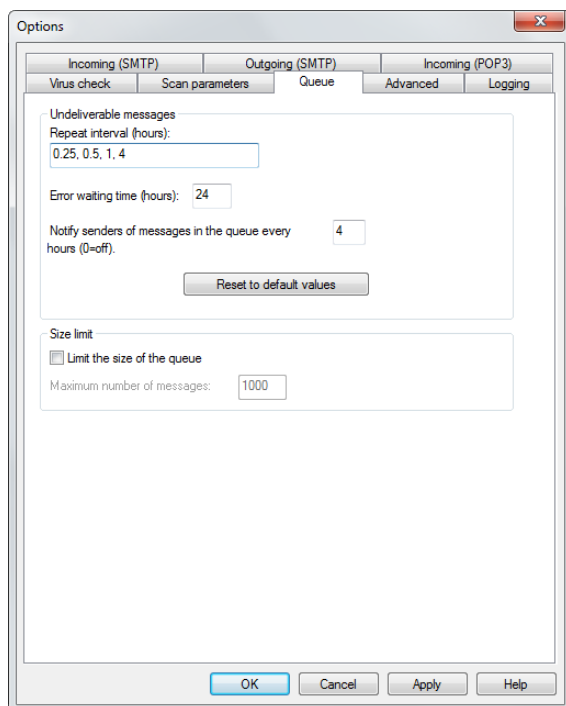
Undeliverable messages

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.

12.2.1.7. Advanced

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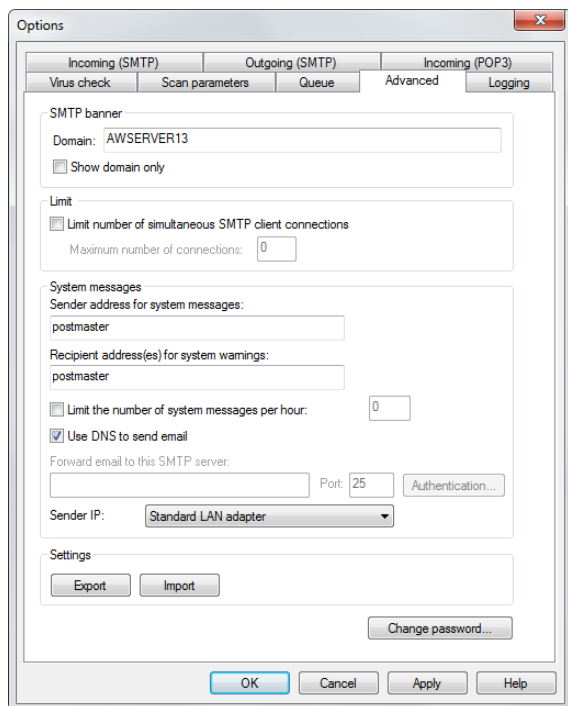
SMTP banner

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 password that you assigned when you started G DATA MailSecurity Administrator 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.

12.2.1.8. 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, located in MailSecurity's installation folder). By selecting **Only junk mail** or **Limit number of emails** you can limit the size of the log file.

12.2.2. Update

The Update window lets you configure G DATA MailSecurity updates. Virus signatures and program files of G DATA MailSecurity can be updated manually or automatically.
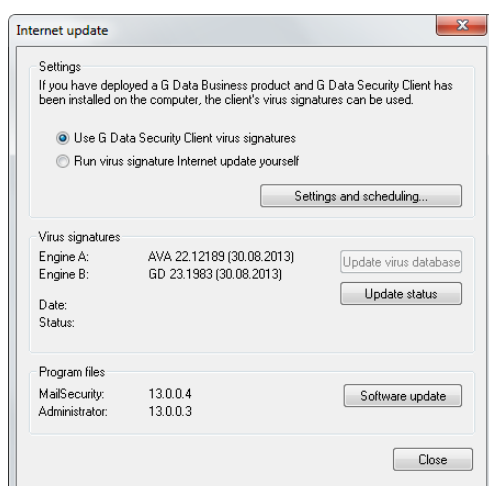
12.2.2.1. Settings

If MailGateway is being operated as part of a G DATA business solution, you can avoid redundant 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 update server will use this data to authenticate you in order to automatically execute the virus signature update.
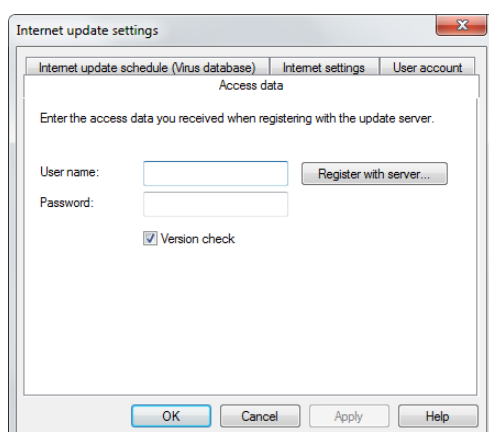
Click the **Register with server** button if you have not yet registered yet. Simply enter the registration number that can be found on your purchase certificate and your customer data and click **Login**. The login data (user name and password) will be displayed immediately. You should write down this 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 (Virus database) 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.
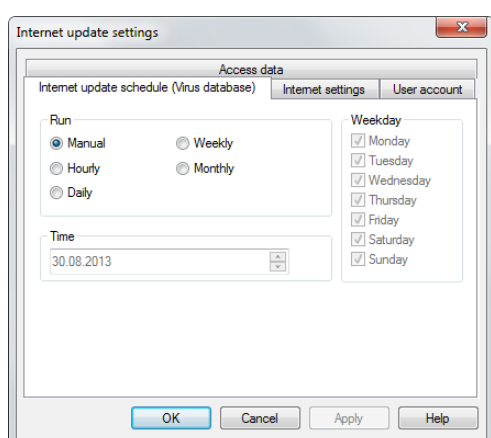
Internet settings
If you use a computer behind a firewall, or if you have other special settings for your Internet access, configure the use of a **Proxy server**. You should change these settings only in case the Internet update does not work. If necessary, ask your Internet Service Provider about the proxy address.
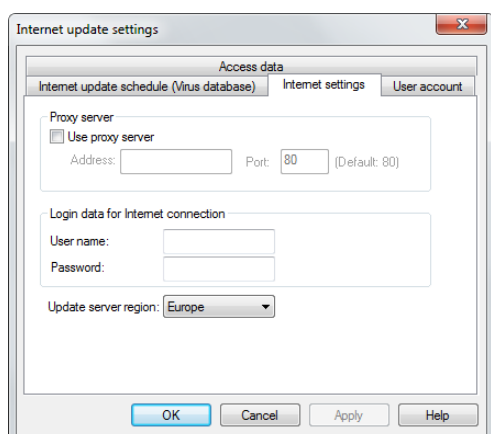
The Internet connection login data (user name and password) are especially important if the automatic Internet update is based on a schedule. Without this information, an automatic connection to the Internet cannot be established. Be sure to enable automatic login in your general Internet settings (for example, for your mail program or web browser). G DATA MailSecurity can start the Internet update process without automatic dialing, 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 mix up the entries you make on the **Access data** and **User account** tabs.
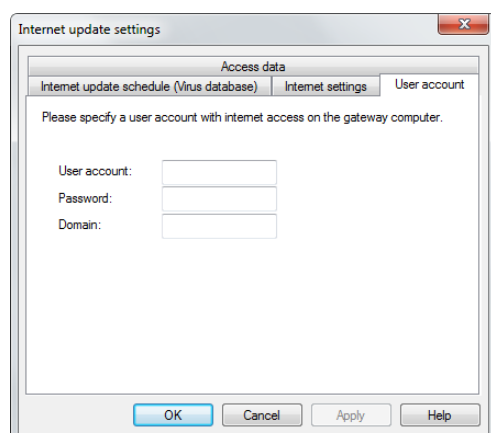
12.2.2.2. Virus signatures

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

12.2.2.3. Program files

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

12.3. 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.

12.3.1. 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 **Options** > **Incoming (POP3)**) and you can configure incoming email processing.

- **Virus scan for incoming email**: Scanning incoming email stops infected mails 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 outgoing 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.
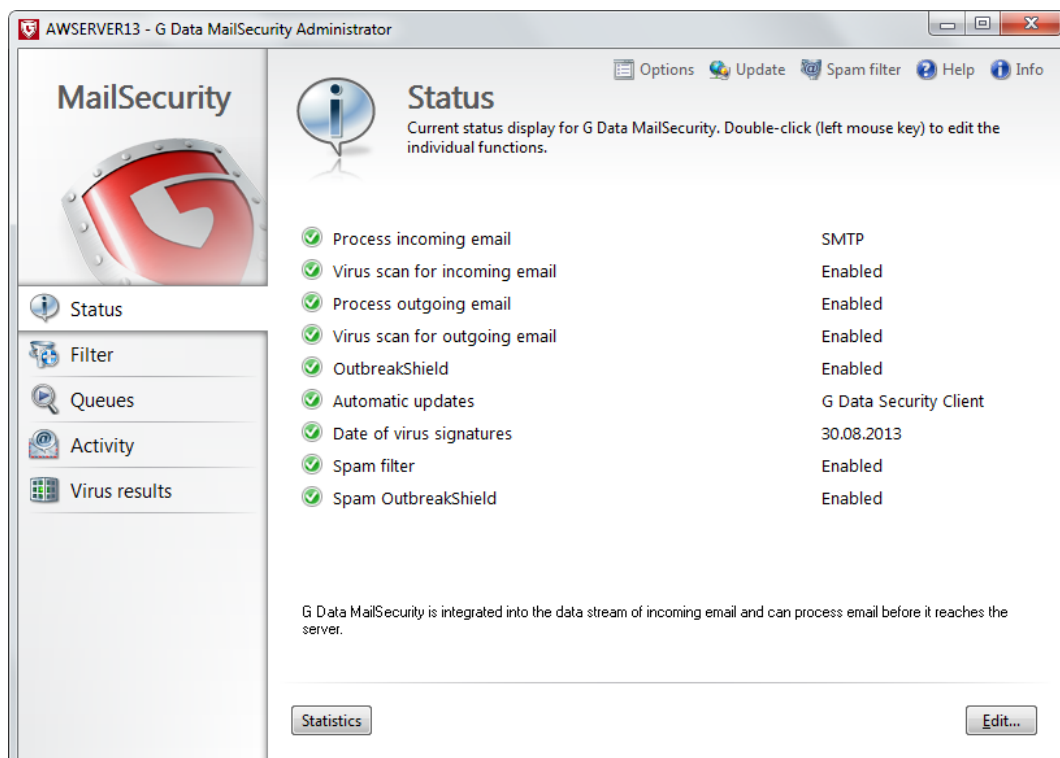
If you installed the option for Statistical assessment, the Status panel will also show a **Statistics** button. It will show statistical information about the mail server and can be configured through **Options** > **Logging**.

12.3.2. 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.
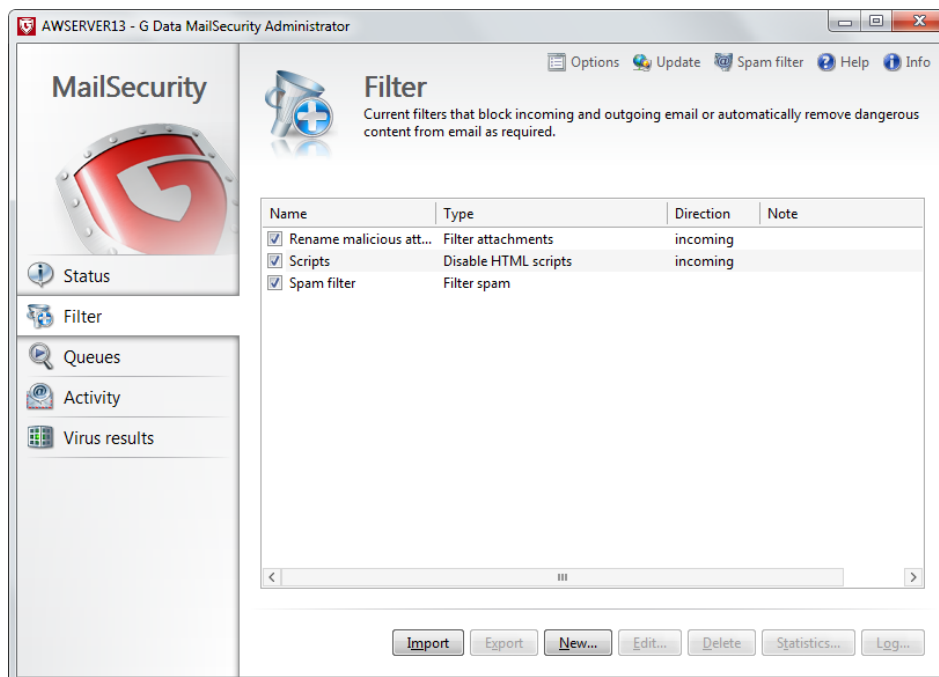
- **Import**: Import filter XML files to restore a backup or reuse filters from other computers.
- **Export**: Individual filters with your settings can be exported as an XML file to be backed up or to be reused on other computers. To export multiple filters, click them while holding the Ctrl key.
- **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 email 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.

12.3.2.1. Filter read receipt

This filter deletes requests for a read receipt for incoming and/or outgoing emails.
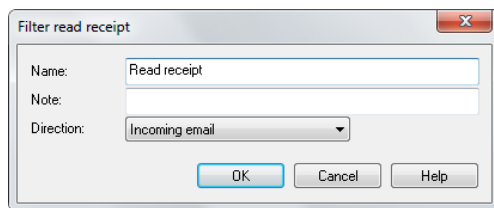
12.3.2.2. Disable HTML scripts

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.
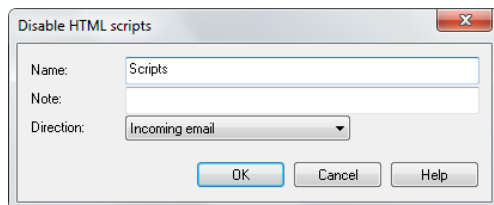
12.3.2.3. Disable external references

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.
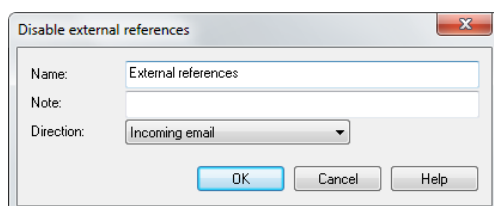
12.3.2.4. Greylist filter

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 (minutes)**: 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 (days)**: 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.
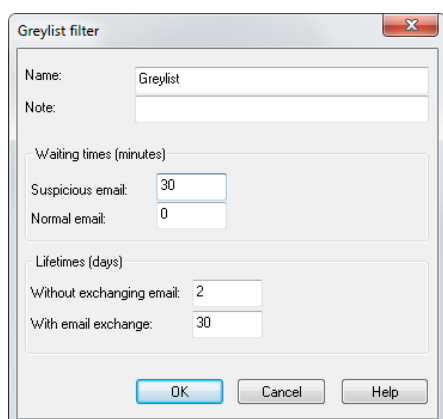
12.3.2.5. Filter attachments

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.
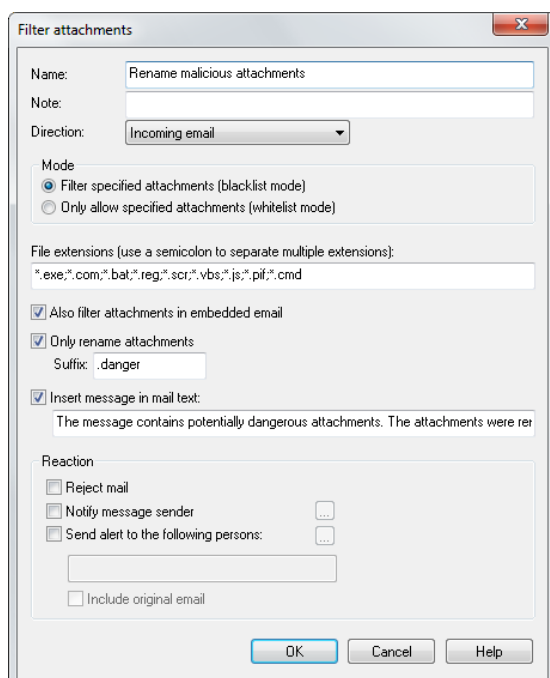
Under **File extensions** you can list the file extensions to which you would like to apply the filter. This lets you list all executable files (e.g. EXE, COM) in one filter, and have another filter for other formats (e.g. MPEG, AVI, MP3, JPEG, JPG, GIF) if their file size would overload the mail server. 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.

12.3.2.6. Content filter

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

> 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).
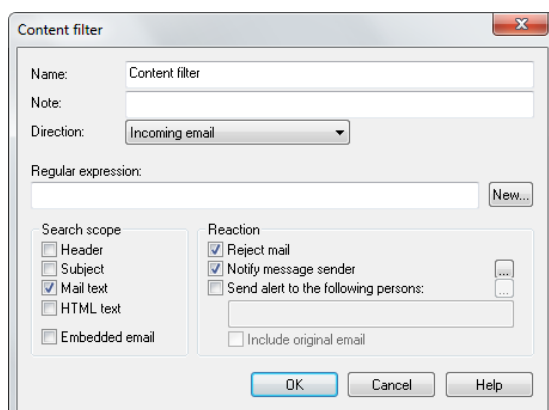
12.3.2.7. Sender filter

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.
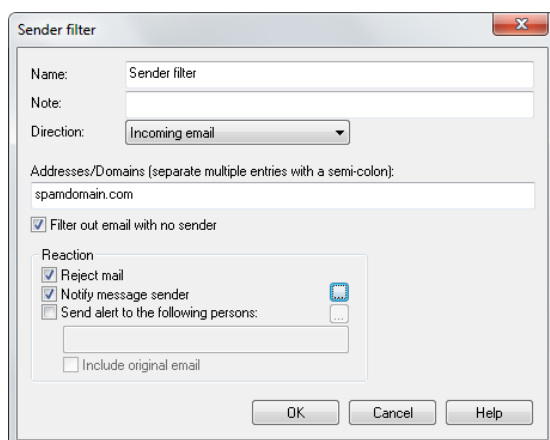
12.3.2.8. Recipient filter

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).
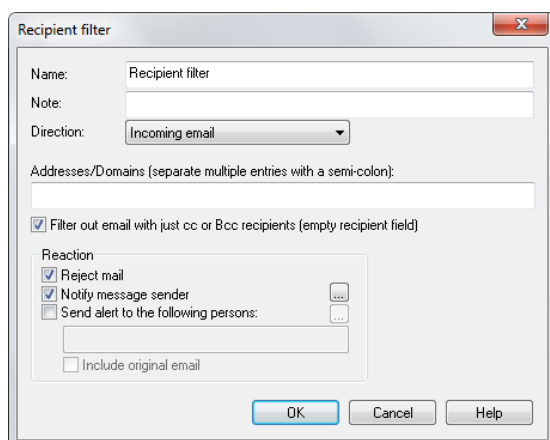
12.3.2.9. Filter spam

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

Filter
You can give an individual name to each filter by entering it in the **Name** field. Add additional information that may be required in the **Note** field. Under **Reaction**, you can define how the spam filter should handle email that may possibly be spam. You can use the spam probability value calculated for the affected email by G DATA MailSecurity to define three different levels of filtering.
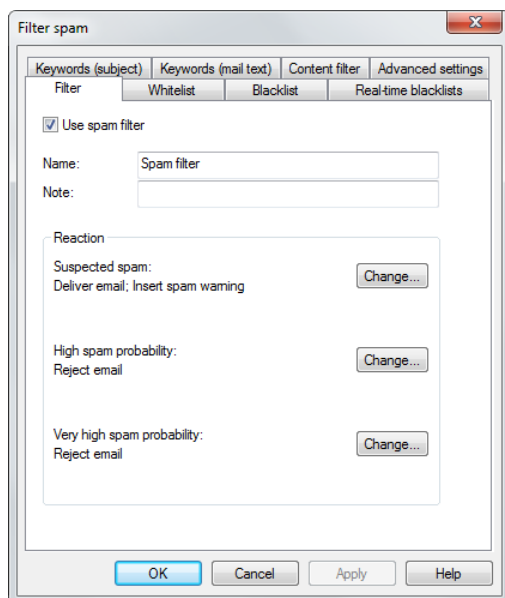
Suspected spam messages, which contain only a few spam characteristics, are not necessarily all spam, but can also be email newsletters or part of a mass emailing that is of interest to the recipient. In such cases, it is recommended that you inform the recipient that the email is suspected spam. **High 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 mail** option allows you to specify that the email does not even reach your mail server. The recipient will never receive this email. You can use **Insert spam warning in mail subject and mail text** to inform the email recipient that the email may be spam. You can use the **Notify message sender** option to automatically send a reply to the sender of the email, in which you can notify the sender that his/her mail has been identified as spam. Since many email addresses are only used once for spam, you should think carefully about using this function. Use **Forward to the following persons** to forward suspected spam emails, e.g., to the system administrator.

Whitelist

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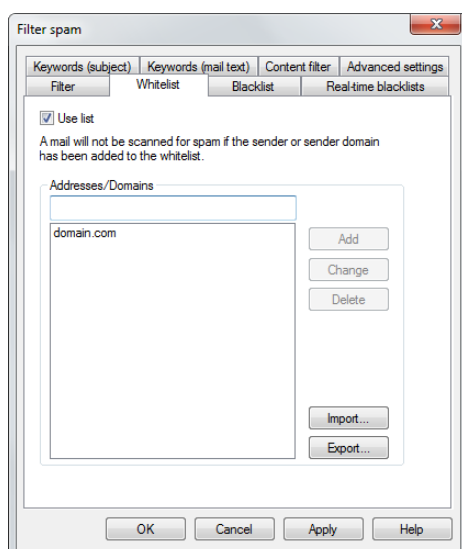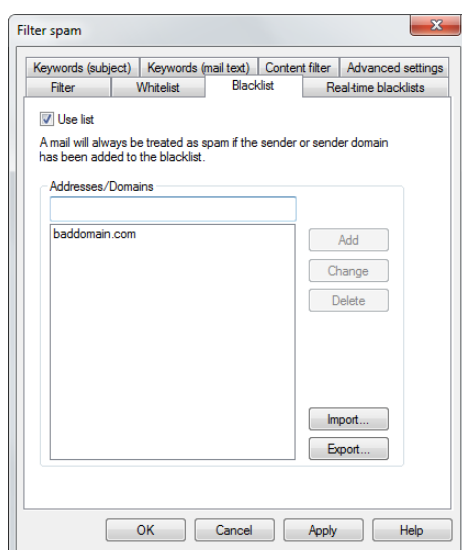
Blacklist

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.

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**.
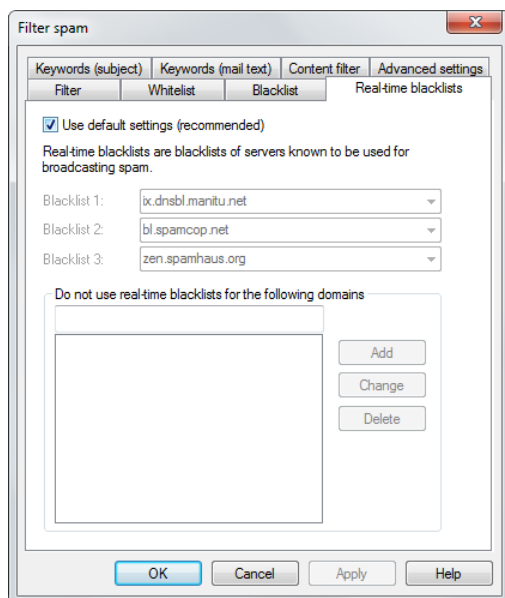
Keywords (subject)

You can 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.
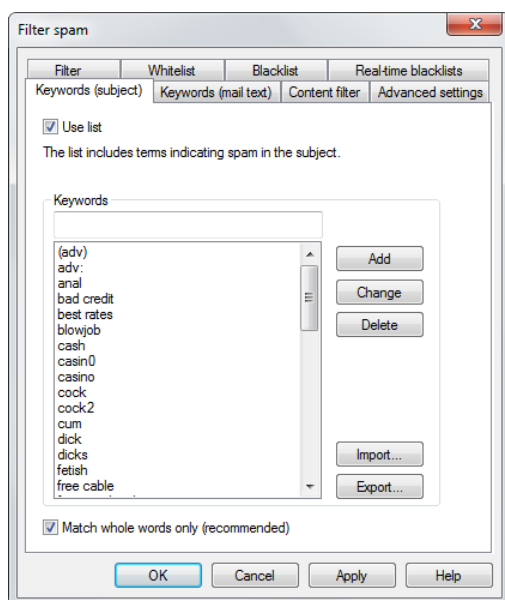
Keywords (mail text)

By defining a list of keywords, you can 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
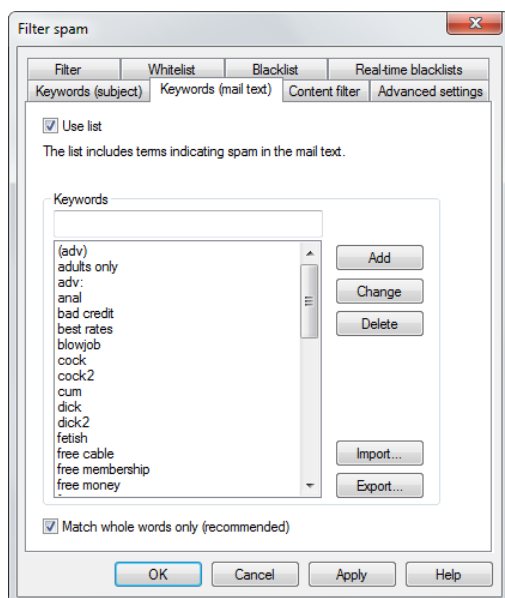
of keywords as a text file. As in the example given earlier, by selecting the **Match whole words only** option, you can have G DATA MailSecurity search the email text for whole words only. So if *cash* has been defined as a keyword, messages containing that word would be suspected as spam, while messages containing *cashew nuts* in the text would not be affected.

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.
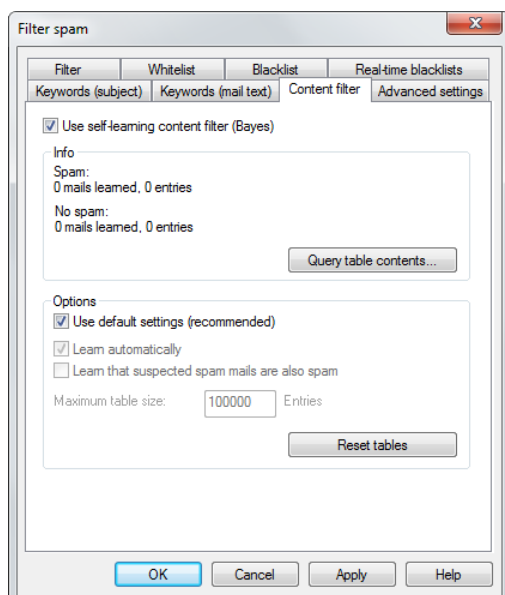
Advanced settings

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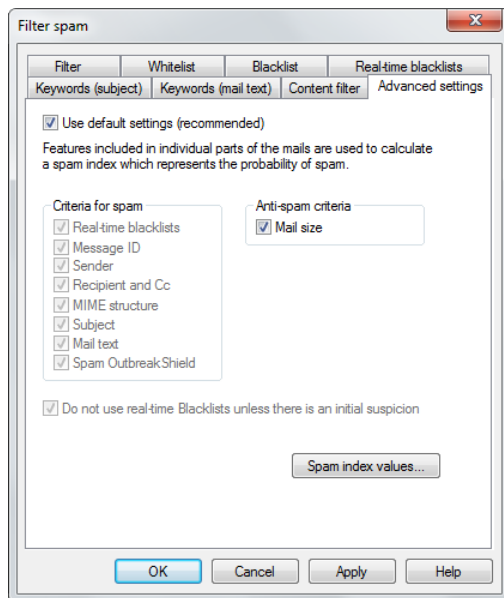
Click **Spam index values** to edit values for the individual attributes that are used to classify emails as Suspected spam, High spam probability or Very high spam probability. It is recommended to leave the option **Use default settings** checked.

12.3.2.10. 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.
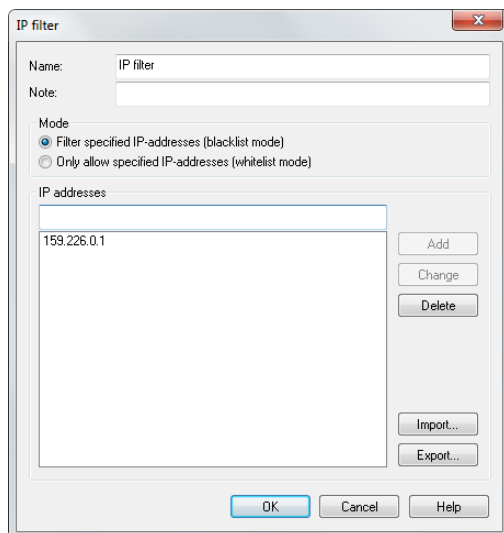
12.3.2.11. Language filter

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.
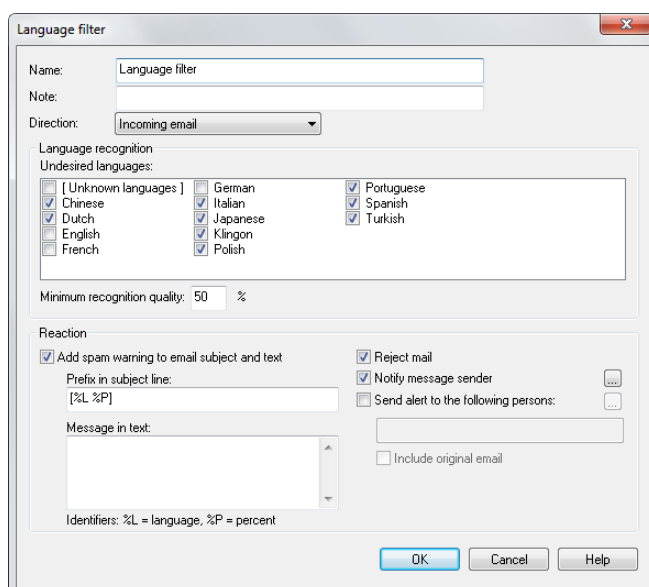
12.3.3. Queues

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 redeliver 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.

12.3.4. 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).

12.3.5. 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.

13. Troubleshooting (FAQ)

13.1. Installation

13.1.1. 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**.

13.1.2. 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**. Click **Online registration** to open the registration form and enter the solution's registration number. You can find the registration number in the order confirmation. In case of doubt, contact your dealer or the relevant distributor.

On entering the registration number, your solution 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 reenter 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 Client Security Business, G DATA Endpoint Protection Business, 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.

13.1.3. MailSecurity for Exchange

13.1.3.1. MailSecurity and Exchange Server 2007

When upgrading MailSecurity for Exchange on Microsoft Exchange Server 2007, Microsoft .NET Framework 3.5 or higher needs to be present. If Microsoft .NET Framework 3.5 or higher is not present, GDVSService will fail to start after the upgrade has been carried out. Installing Microsoft .NET Framework 3.5 or higher before or after upgrading MailSecurity for Exchange will ensure full functionality.

13.1.3.2. Updating version 12

Due to changes in the installation procedure, MailSecurity for Exchange installations that were initially deployed at version 12 cannot be updated to version 14, even if they have previously been

updated to version 13.0 or 13.1. In that case, the previous version of MailSecurity for Exchange should be uninstalled before installing version 14. In addition, it should be ensured that MailSecurity for Exchange is installed on all Exchange servers that are running the Mailbox or Hub Transport roles.

13.1.3.3. 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.

13.1.3.4. Installation in a network with multiple Domain Controllers

When installing MailSecurity for Exchange in a network with multiple Active Directory Domain Controllers, the setup wizard requires the tool Repadmin.exe to be present. Repadmin.exe is available as part of the Active Directory Domain Services role, the Active Directory Lightweight Directory Services role and the Active Directory Domain Services Tools (Remote Server Administration Tools). Before starting the installation wizard of MailSecurity for Exchange, make sure one or more of these components are present.

13.2. Error messages

13.2.1. 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 **Security events** module. Delete the report and download the current update of the program files (G DATA Security Client) from the G DATA update server. Subsequently, perform an update of the program files on the affected clients. Please contact our **support team** if the error occurs again.

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

13.2.3. "Microsoft Exchange Server 2007 SP1 is required to install G DATA MailSecurity"

If you receive the error message "Microsoft Exchange Server 2007 SP1 is required to install G DATA MailSecurity", 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**.

13.3. Linux clients

13.3.1. Installation

The installation of G DATA Security Client for Linux and G DATA Security Client for Mac uses a ManagementServer-based repository. When deploying a Linux or Mac client, the relevant binaries will

be copied from the ManagementServer repository to the client. If they are not yet available in the repository, they will be downloaded from the G DATA update servers, added to the repository on the ManagementServer and subsequently deployed to the client.

13.3.2. Background processes

To check whether both G DATA Security Client for Linux processes are running, enter the following in a terminal window:

linux:~# *ps ax/grep av*

The response should contain the following processes:

/usr/local/sbin/gdavserver
/usr/local/sbin/gdavclientd

You can start the processes with:

linux:~# */etc/init.d/gdavserver start*
linux:~# */etc/init.d/gdavclient start*

You can stop the processes with:

linux:~# */etc/init.d/gdavserver stop*
linux:~# */etc/init.d/gdavclient stop*

To do this, you must have root permissions.

13.3.3. Log files

Remote installations of G DATA Security Client for Linux are logged in /var/log/gdata_install.log. The gdavclientd process logs information and errors to /var/log/gdata/avclient.log. The gdavserver process logs information and errors to /var/log/gdata/gdavserver.log, which helps troubleshooting the connection to G DATA ManagementServer.

> If you wish to see more information, edit the configuration files /etc/gdata/gdav.ini and /etc/gdata/avclient.cfg and set the *LogLevel* to value *7* (adding it if it does not exist yet). 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.

13.3.4. Scan server test

Use the **gdavclientc** command line tool to test the functioning of the gdavserver scan server. Version information can be retrieved using the *baseinfo* and *coreinfo* commands. Run a test scan using the *scan:<path>* command. See the chapter **gdavclientc** for more details.

13.3.5. Connection with G DATA ManagementServer

Communication with G DATA ManagementServer is configured in /etc/gdata/avclient.cfg. Check whether the IP address of ManagementServer was entered correctly. If not, delete the incorrect entry and enter the IP address of ManagementServer directly or re-enable the Linux client via G DATA Administrator.

13.4. Other

13.4.1. 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.

13.4.2. 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 **Quarantine: move back**. Please contact our support team if moving back fails.

13.4.3. Connect to ManagementServer via its IP address instead of its name

The server name will be requested during the installation, but can be replaced by the IP address if you want to connect to the ManagementServer via its IP address instead of its name. You can also replace the server name with the IP address after G DATA ManagementServer has already been installed. To do this, edit the file Config.xml (located in the installation folder of G DATA ManagementServer) and change the value for *MainMms* to the IP address. More information about Config.xml can be found in the Reference Guide.

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 installation medium, the installation program asks for both the server name and the name of the computer. Enter the appropriate IP address here.

13.4.4. Default 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/Server 2008 and newer: C:\Program Files (x86)\Common Files\G DATA\AVKScanP

\BD or G Data

G DATA ManagementServer virus signatures:

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

- Windows Vista/Server 2008 and newer: C:\ProgramData\G DATA\AntiVirus ManagementServer \Updates

G DATA Security Client quarantine:

- Windows XP/Server 2003/Server 2003 R2: C:\Documents and Settings\All Users\Application Data \G DATA\AntiVirusKit Client\Quarantine

- Windows Vista/Server 2008 and newer: C:\ProgramData\G DATA\AntiVirusKit Client\Quarantine

G DATA ManagementServer quarantine:

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

- Windows Vista/Server 2008 and newer: C:\ProgramData\G DATA\AntiVirus ManagementServer \Quarantine

G DATA ManagementServer databases:

Windows Vista/Server 2003 and newer:

- C:\Program Files (x86)\Microsoft SQL Server\MSSQL12.GDATA2014\MSSQL\Data \GDATA_AntiVirus_ManagementServer_*.mdf

- C:\Program Files (x86)\Microsoft SQL Server\MSSQL12.GDATA2014\MSSQL\Data \GDATA_AntiVirus_ManagementServer_log_*.ldf

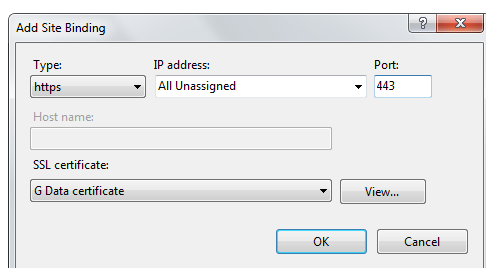## 13.4.5. How do I enable an SSL Server Certificate in IIS 7 and higher?

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 higher (Windows Vista/Windows Server 2008 and newer), 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*.

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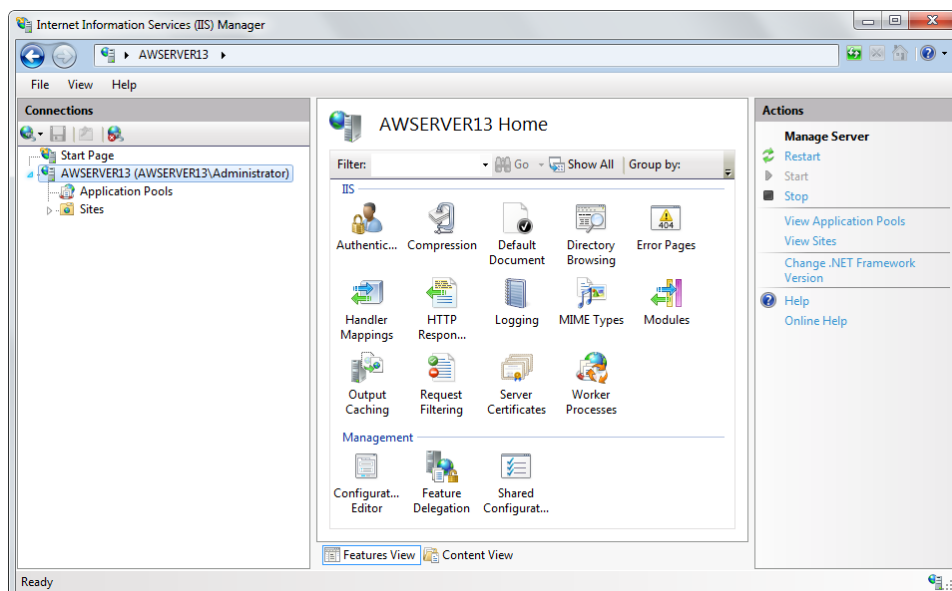
To apply the certificate to site communication, select the appropriate site in the **Connections** panel. On the **Actions** panel at the right, choose **Bindings**. Click **Add** to add a new binding. Select https as **Type** and select the certificate you just added in the **SSL certificate** dropdown.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

13.4.6. 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).
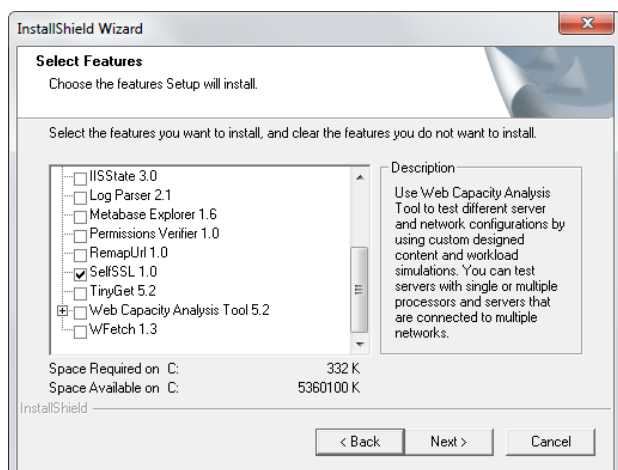
To enable an SSL Server Certificate in IIS 5 (Windows XP) or IIS 6 (Windows Server 2003), you can use

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** > **Programs** > **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.

14. 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