G DATA Administrator Module

G DATA Administrator 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.

Client Modules

Client Dashboard

The Dashboard area provides you with information about the current state of the clients in the network.

G DATA Security Status
Under G DATA Security Status you can set all the basic security settings for the clients or groups you have selected in the Clients section. By clicking on the respective entry, you can perform actions here directly or switch to the respective task area. As soon as you have optimized the settings of a component with the attention symbol, the symbol in the status area changes back to the green symbol. For a quick detailed overview, the Clients - Overview is more suitable.

Client Connections

The Client Connections section provides a time-based overview of the connections that the respective clients have had with G DATA ManagementServer. Care should be taken to ensure that all clients connect to G DATA ManagementServer on a regular basis. To better control the connections, each client sends a heartbeat every hour. If this fails, the client is probably offline. If the heartbeat is sent, but the client does not update the virus signature updates, for example, there is a communication failure.

Clicking on the pie chart takes you to the client overview, where the security status is already pre-filtered according to the selected area.

Top 10 Clients - Warnings

The Top 10 Clients - Warnings overview helps to find problematic clients. The chart shows the clients with the most virus reports. While G DATA successfully fends off these infections, the fact that certain clients are often attacked by malware may indicate problems. Perhaps one of the other protection mechanisms is misconfigured, or the end user is particularly at risk due to targeted malware attacks or careless (surfing) behavior. Here, the client's security configuration should be checked. If the end user's (mis)behavior is a possible cause, PolicyManager policies can be used to restrict access to dubious resources.

Clicking on the displayed client name takes you directly to the security events for this client.

Report Status

The chart shows infections, errors, and Firewall and PolicyManager requests. Excessive errors from any of the modules or other notable spikes in the graph can be checked via the individual reports in the Security Events module.

Module Clients

- Clients - Overview
- Clients - Software
- Clients - Hardware
- Clients - Messages

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.

Clients - 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:

- **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).
- **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**

You can display various columns in the overview, for more tips and explanations on operation, see G DATA Administrator Controls.

The **Heartbeat** is a tool to find communication failures. If the Heartbeat fails, the client is switched off or has no network connection, for example. If the Heartbeat is present but the client is not loading signature or program updates, there is a communication problem with the ManagementServer.

The Heartbeat is always activated from version 15.1. It is displayed when it is selected in Select columns.

Right-clicking on a client gives you the following options

- **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**.
- **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.
- **Remove Authorization** As of version 15.1, it is possible to remove the authorization of a client.
- **Properties** (only in the context menu): Display properties for the selected client (**General, Network info, Security risks** and **Hardware**).

Clients - 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.

Clients - 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**

Clients - 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.

Module iOS clients

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.

Module iOS settings

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

iOS-settings - 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.

iOS-settings - 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.

iOS-settings - AntiTheft

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)**.

Unable to render {include} The included page could not be found.

Module Sendmail and Postfix

- Sendmail/Postfix - Settings
- Sendmail/Postfix - AntiSpam

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.

Sendmail/Postfix - 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).

Sendmail/Postfix - 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.

Module 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.

Module Client settings

- Client settings - General

- Client-settings - Monitor
- Client-settings - Email
- Client-settings - Web
- Client-settings - AntiSpam

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.

Client settings - 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, alware-related information is sent to the G DATA SecurityLabs.

Signature update settings

Define where clients obtain their virus signature updates:

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

Proxy server

Specify which proxy settings the client or group should use.

If enabled, the user can use their own proxy settings, but this should only be allowed in exceptional cases. Enabling the option may compromise the security of the client.

The proxy server can also be configured differently from the system-wide settings without applying the user's proxy settings.

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.
- A**llow the user to change email options**: If this function is enabled, the client user has the option to change the Email and Anti Spam 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.

Client-settings - 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. :\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.

Client-settings - 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.

Outlook protection

Outlook Protection enables email scans in Outlook using an integrated plug-in.

Protect Microsoft Outlook with an integrated plug-in: When this function is activated, a new function called **Scan folder** for viruses is added to the client's Outlook in the **Tools menu**.

Regardless of the G DATA Administrator settings, the user of the individual client can scan the currently selected mail folder for viruses. **Right-click** on the folder to be scanned. Select **G DATA** at the bottom of the menu and then **Check for viruses**.

Client-settings - 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.

Client-settings - 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**.

Module Exchange settings

- Exchange settings - General

- Exchange-settings - AntiSpam

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, 2013, 2016 or 2019.

Exchange settings - 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.

Exchange-settings - 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.

Unable to render {include} The included page could not be found.

Module Tasks

- Tasks - Single scan job
- Tasks - Periodic scan job
- Tasks - Backup jobs
- Tasks - Restore jobs
- Tasks - Patch applicability jobs
- Tasks - Software distribution jobs
- Tasks - Rollback jobs

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.

Tasks - Single scan job

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).

Tasks - Periodic scan job

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).

Tasks - 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.

Tasks - 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 B**ackup 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.

Tasks - 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.

Tasks - 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 manage d 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 nextboot.
- **Immediat ely after logging in**: The software distribution job will be run after the next time anend 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.

Tasks - 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.

Module 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 comp rehensive 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.

PolicyManager - 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 admini strator 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 specificfile 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 filename 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).

PolicyManager - 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 (**R ead** / **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 except ion, 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).

PolicyManager - 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 c osts 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 **Addr ess** (without protocol) and click **OK** to add the exception. Click Edit to edit an existing exception or **Delete** to delete exception(s).

PolicyManager - 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 theavailable controls to specify the quota available for Internet usage. Daily, weekly or monthly quotas can be issued; for example, the specification 0420:05 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 atime 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 **Bloc k 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.

Module Firewall

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

Firewall - 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 applicat ions**: If the client computer is connected to G DATAManagementServer, 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 theManagementServer 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:
  - **Autopilot mode** (see **Firewall** > **Overview** > Settings).
  - 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.

Firewall - 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.

Firewall - 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.

Firewall - 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.

Firewall - 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 orenabling 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**

Module 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.

PatchManager - 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).

PatchManager - 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.
  - **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.
  - **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.

PatchManager - 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**).

Module 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.

Logs - 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.

You can customize the table to display more or fewer columns. For instructions on how to do this, see G DATA Administrator controls.

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.
- **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.

Release blocked applications

Users can request a share for blocked applications, which will appear in the security events.

To share an application, click the **Application(s) blocked** entry.

Select the **type of sharing** and confirm it with **Perform action**.

You can still enter a message text or use the standard text.

If you want to activate the application for several users, but not all users should see the message, then enter the user who should receive the message under User Name (optional).

Confirm your entries with **OK**.

Comments can be written for the safety events.

The comment column can be displayed via Select columns.

A comment can be written by double-clicking in the comment column. Alternatively, right-click on the line to open the menu and select Edit comment.

A free text field opens. When a comment is opened later, the history for the entry is displayed.

Logs - 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**

Module 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**.

ManagementServer Modules

Module Server

Server - 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 - 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**.

Server - Tenant management

The system administrator may create additional user accounts for the G DATA administrator interface in the following way:

Klick **Add** and enter the **Tenant**, a **Unique identifier**, the corresponding **User** and a **Description**, if necessary.

The green plus sign allows for the quick creation of a new user account, for which you need to choose **User name**, **Account type**, **Permissions** and a **Password**.

After the creation of a tenant a new, correspondingly named node in the **Clients/ManagementServer panel** is established which contains a base structure similar to a fresh installation. The previously existing structure with the existing clients is transferred to the **Standard** node. Clients can be moved from the Standard node to the new tenant.

Beware: The client names need to be unique among all tenant nodes! It is for example not possible to have a client with the name "PC-WORKSHOP" both in tenant A and tenant B.

Modules and options that can be configured individually for each tenant will display a drop-down menu to choose the tenant for which the option is to be set. In this way, individual **Reports** or recipients for **email notifications** can be defined.

The creation of an **Installation package** also allows for the selection of the tenant, and the newly installed client will be integrated into the proper tenant node immediately.

To **sign in** to G DATA Administrator with a tenant account, select **Integrated authentication** in the login screen. The **Clients/ManagementServer panel** will then only display the node of that tenant, and it is not possible to access any other tenant node or the Standard tenant.

Using a tenant account does not allow the usage of any ManagementServer modules except the **ReportManager**.

Furthermore, the following G DATA modules and components cannot be used in combination with the Tenant management:

- Search for computers in the **Server setup wizard**
- **Active Directory** sync
- Deployment of **Subnet-ManagementServers**
- **Backup**
- **PatchManagement**

Server - 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**.

As of version 15.1, failed login attempts to G DATA Administrator are displayed with the username and IP address entered.

Module General settings

General settings - Cleanup

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

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

General settings - Synchronization

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

- **Clients**
  - **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.
  - **Notify client if settings have been changed on the server**: Tick this setting to notify clients immediately of new settings, regardless of synchronization interval.
  - **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**
  - **Interval for synchronizing**: Define the interval for synchronization between main ManagementServer and subnet server(s).
  - **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**
  - **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.
  - **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.

General settings - 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.

General settings - 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 pen 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.

General settings - 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.

Module Updates

- Updates - Signature updates
- Updates - Program updates
- Updates - Staged distribution
- Updates - Access data and settings
- Updates - Signature rollback

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**.

Updates - 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.

Updates - Program updates

In the Program Updates section, you configure the download of client program files from the G DATA update server to ManagementServer. Program file updates should be installed automatically so that all clients can use the full scope of G DATA CyberDefense products.

The following information and settings are displayed under **Program Files (Client)**:

- **Current version**: The current version of the client program files stored on the ManagementServer.
- **Last run**: The last run of the update process.
- **Status**: The status of the update process.
- **Update Status**: Updates the status.
- **Start update now**: Starts an immediate update of the client program files on G DATA ManagementServer.

In the **Automatic updates** section, you can schedule the update of client program files. The settings are identical to those under Signature updates.

G DATA ManagementServer itself can only be updated via a Start menu item. To do this, call up the **Internet Update** entry in the G DATA ManagementServer program group in the Start menu.

Program file updates are not issued every hour, so the update interval can be set to a daily or weekly request. Scheduling program file updates is also recommended for servers that are not permanently connected to the Internet. The Internet connection option will only perform an update if G DATA ManagementServer detects that the server has an Internet connection. The only reason not to have program files updated automatically by G DATA ManagementServer is if the Internet connection is not always available. To prevent files from being automatically distributed to clients, appropriate configurations are required in the Client Settings module.

A program update can also be started manually on the client. Proceed as follows:

Clients > **Clients** > **Overview** > search/filter desired clients in the list > **right click** on the clients > **Update program files now**

⚠ Program file updates always require a reboot of the client computer.

MailSecurity for Exchange

As with G DATA Security Client, MailSecurity for Exchange performs an automatic upgrade when a new version is available on ManagementServer. To ensure that the latest version of the Exchange plug-in is used, the Internet Update tool of ManagementServer has the Update program files (client) feature. If the Exchange plug-in updates its program files automatically according to the configuration, this will be done the next time it connects to the ManagementServer. Alternatively, an upgrade can be performed manually using G DATA Administrator.

Updates - Staged distribution

In the **Staged distribution** area, you can specify whether to apply program updates to all clients simultaneously or in stages. A staged distribution reduces the server and network load that occurs during a program update.

If you choose staged distribution, you can specify whether the distribution is automatic or you can specify yourself which clients are to receive program updates first, which clients come after, and the extent to which the distribution is subdivided into different distribution stages.

The first level always includes five clients.

If you do not want to use staged distribution, it is possible to disable the automatic program update option within G DATA Administrator and then distribute it via the context menu on a group or individual basis.

To do this, select the desired client or client group. **Right-click** to open the menu. Click on **Update program files automatically** to remove the check mark and thus disable the automatic program updates.

Alternatively, you can also make the settings via the client settings General under Updates.

Updated client software may need to be tested to ensure compatibility with all client configurations on the network. Although minor version changes usually have no side effects, a staged rollout is recommended. Staged distribution can be enabled in the Updates module. Only when the program file has been successfully updated on the clients of one stage, it will be installed on the clients of the next stage.

The number of stages can be defined manually. The larger the network, the more stages are recommended to ensure a smooth installation. It is also possible to configure after how many days the next stage is updated. With the default value of three days, clients can be checked for problems to stop the distribution of a particular update if serious problems occur. The staged distribution settings can be changed by editing the Config.xml configuration file.

⚠ Program file updates always require a reboot of the client computer.

For some client roles, this must be carefully planned so that the computer is not restarted during an important task. In these cases, the Restart after update setting controls client behavior. The end user can be notified that their computer needs to be restarted. This restart can be forced or a report can be generated in the Security Events section so that the administrator can manually intervene and restart the computer at a later time.

Updates - 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: **https://dlarray-europ-pool-1.gdatasecurity.de/api/status**. 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).

Updates - 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.

Modul ReportManager

The ReportManager creates reports with information from various areas of the G DATA security solution. The reports are sent by e-mail to selected recipients, but can also be accessed directly via G DATA Administrator.

Export nach CSV	Export the list as a CSV file
	Update the table
	Remove selected report
	Create new report
Import	Import existing configurations (.dbdat)
Export	Export Report Settings as .dbdat

You can call up all reports that have already been sent by clicking on the plus sign on the left in the overview. You can see the date and time when the respective report was created and sent. Double-click on the date to open the respective report in G DATA Administrator.

Right-click on the report to open the menu to perform the following actions:

Update	Update the table
Remove	Remove selected report
Duplicate	Create a copy of the selected report

Execute immediately	Immediately receive the selected report. To view it, click on the plus sign on the left and then double-click on the entry with the current date.
History	In a larger overview window you can see all the reports that have been sent. Double-click on the date to open the respective report.
Properties	Opens the report definition. Among other things, you can adjust the time of execution, recipient and modules.

The G DATA Defense Report cannot be edited or deleted. However, it can be duplicated for editing.

Create or edit a new report

Module 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.

Module 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**.