G DATA
INTERNET SECURITY
FOR ANDROID™

USER MANUAL

G DATA

TRUST IN
GERMAN
SICHERHEIT

1. Introduction

G DATA INTERNET SECURITY FOR ANDROID offers comprehensive protection against malware, intrusive apps and phishing attacks. Locate lost devices or wipe their content remotely to prevent unauthorized access. The all new phishing and web-protection uses the latest cloud technology to detect and wipe out even the most current threats. All this combined in a modern and intuitive interface, so you can stay focused on your real tasks while on the go.

2. Installation

In order to install G DATA INTERNET SECURITY FOR ANDROID, make sure that your Android device has been configured to allow apps from outside Google Play to be installed. This option can be enabled as follows:

- Open the **Settings** app.
- Tap the **Security** option.
- Enable the option **Unknown sources**.

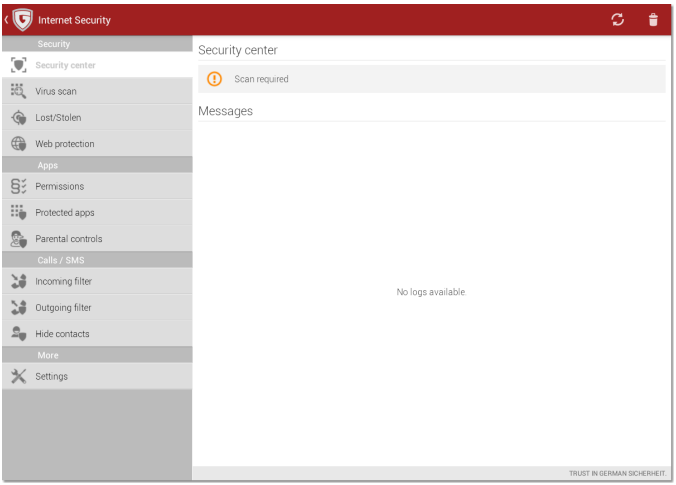
After enabling the installation of apps from outside Google Play, open the device's browser and enter the URL **gms2.gdatasoftware.com**. Once the download has been completed, you can install the app by tapping the download's notification. After the installation finishes, start the app and enter your license key by tapping **Activate updates**.

3. Security

3.1. Security center

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

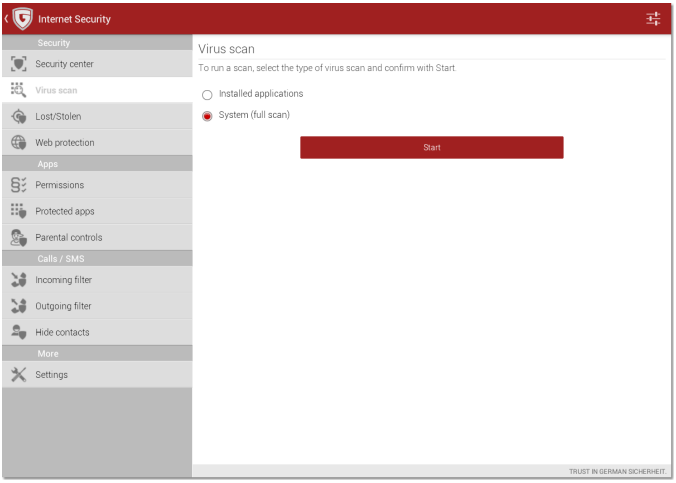
In the top right corner, select the update symbol to download the latest virus signatures. The bin symbol lets you remove all reports listed under **Messages**.



3.2. Virus scan

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

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



Select the settings symbol in the top right corner to open the **Virus scan** settings.

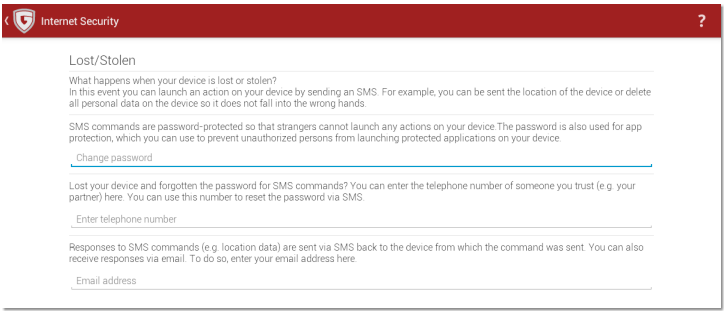
3.3. Lost/Stolen

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

The first time you open the **Lost/Stolen** menu, you will be prompted to configure several settings:

- **Password**: A numeric PIN code that needs to be entered with every SMS command. The password is also used for **Protected apps** and **Parental controls**.
- **Telephone number** (optional): Only from this phone number will you be able to remotely reset the password. If you activate any of the **Theft detection** options, an SMS containing the device's location will be sent to this phone number.
- **Email address** (optional): Responses to SMS commands (e.g. location data) are sent by SMS to the device from which the command was sent. Optionally, they can be sent to an email address as well. If you activate any of the **Theft detection** options, an email containing the device's location will be sent to this email address.

Use the settings symbol in the top right corner if the settings need to be changed afterwards.

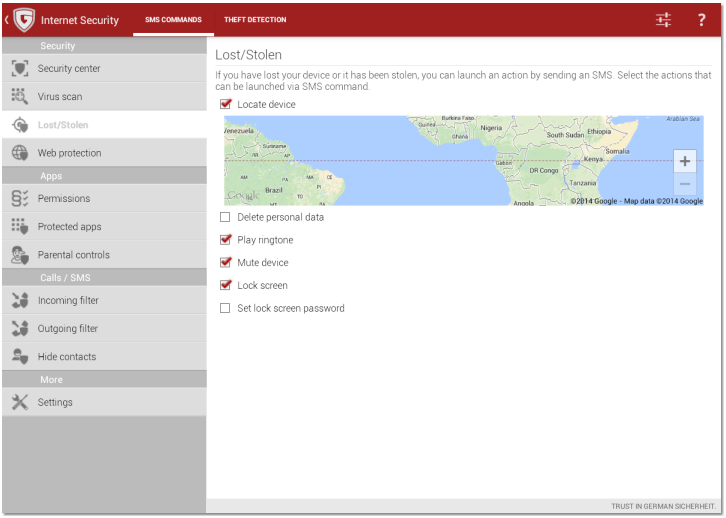


3.3.1. Permitted SMS commands

To protect lost or stolen devices, various measures can be remotely activated by sending an SMS message containing the appropriate command as well as the password which was defined in the **Lost/Stolen settings**. Responses to SMS commands (such as location data) are sent to the phone number from which the command was issued.

The **Permitted SMS commands** module lets you define which commands will be accepted by the device. The following options are available:

- **Locate device:** The device will report its location via SMS. If an email address has been entered in the **Lost/Stolen settings**, location data will be sent there as well. To trigger this function, send an SMS containing the text *password* **locate**.
- **Delete personal data:** The device will be reset to its factory settings. All personal data will be wiped. To trigger this function, send an SMS containing the text *password* **wipe**.
- **Play ringtone:** The device will play a ring tone until INTERNET SECURITY FOR ANDROID is started. This will assist in locating lost devices. To trigger this function, send an SMS containing the text *password* **ring**.
- **Mute device:** If you do not want the device to call attention to itself with ring tones or other signals, it can be muted. This does not include the ring tone that is used to locate lost devices. To trigger this function, send an SMS containing the text *password* **mute**.
- **Lock screen:** The device screen can be locked to prevent the device from being used. To trigger this function, send an SMS containing the text *password* **lock**. If no lock screen password has been set, the SMS command password will be used.
- **Set lock screen password:** Set a password to unlock the device if the lock screen feature has been enabled. To trigger this function, send an SMS containing the text *password* **set device password:** *devicepassword*. Make sure to send the lock command to lock the device after setting the password.



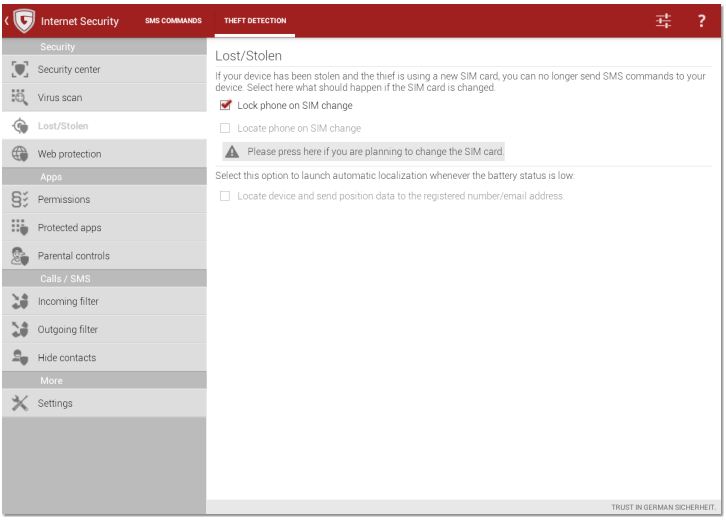
To remotely reset the password, send an SMS from the phone number that you specified in the **Lost/Stolen settings** containing the text **remote password reset:** *newpassword*.

Information about the SMS commands can be accessed by tapping the question mark symbol in the top right corner.

3.3.2. Theft detection

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

- **Lock phone on SIM change**: Same functionality as the option **Permitted SMS commands** > **Lock screen**.
- **Locate phone on SIM change**: The device will report its location by sending an SMS message to the phone number and/or email address that was defined in the **Lost/Stolen settings**.

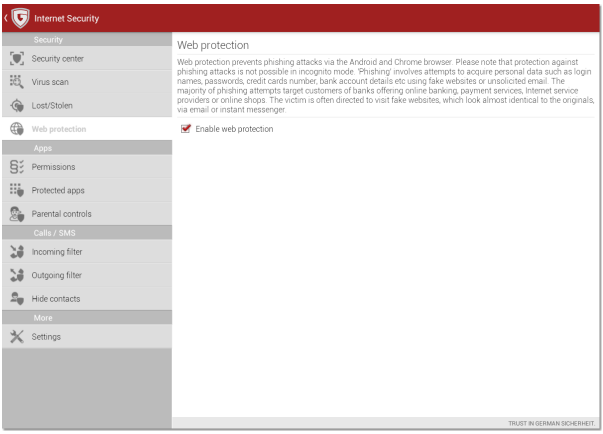


If you need to change the SIM card yourself, use the option **Please press here if you are planning to change the SIM card**. It will temporarily disable the SIM change detection until the device is rebooted.

When the battery level is low, the device will no longer automatically detect its location using GPS signals. Select **Locate device and send position data to the registered number/email address** to enable reporting of its last known location whenever the device enters power saving mode.

3.4. Web protection

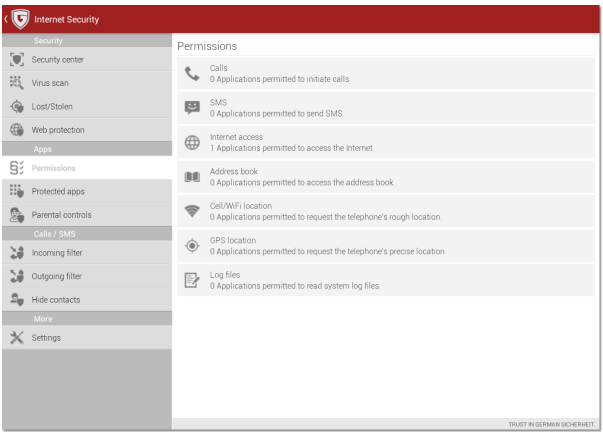
The **Web protection** module prevents phishing attacks. It blocks phishing websites from being opened in the Android browser and in Chrome. To minimize data traffic when using a mobile network, the **Web protection** module can be configured to only look up websites when there is WLAN connectivity (see **Settings** > **Web protection**).



4. Apps

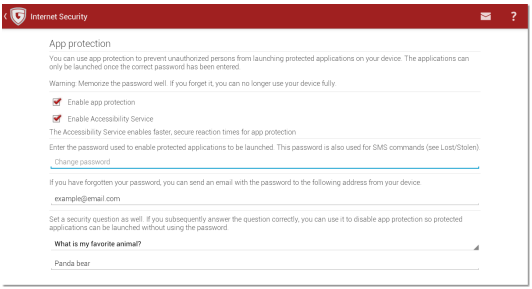
4.1. Permissions

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



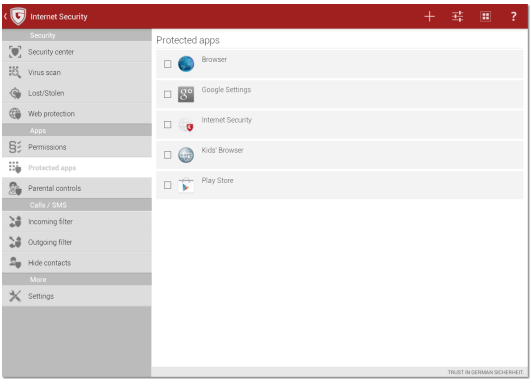
4.2. Protected apps

Protected apps allows you to block certain apps from being used on the device. Using password protection, apps like Play Store can be blocked. The first time you open the app protection module, you will be prompted to configure several settings. Afterwards, the settings can be changed at any time by tapping the settings symbol in the top right corner of the apps list.



- **Enable app protection**: Enable password protection for apps.
- **Enable Accessibility Service** (recommended): Enable a background service that provides faster reaction times.
- **Password**: A numeric PIN code that needs to be entered in order to run a protected app. The password is also used for **Permitted SMS commands** and **Parental controls**.
- **Email address**: Password recovery emails will be sent to this address.
- **Security question**: Define a security question and answer. If you forget your password, you will be asked to provide the answer in order to disable app protection.

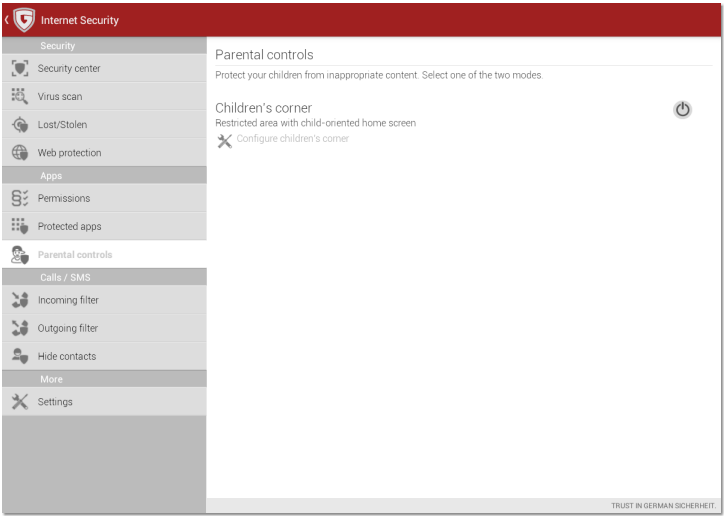
Using the email symbol in the top right corner of the settings window, you can verify the entered email address by sending a test email.



To add password protection to an app, tap the plus symbol in the top right corner. You can select apps using different views: **Recommended**, **Downloaded**, and **All**. Select one or more apps and tap **Done** to add them to the list. The apps are automatically protected, requiring users to enter the password when they are launched. To remove one or more apps from the list, select them and tap **Done** in the top left corner.

4.3. Parental controls

Using **Parental controls**, you can make sure that your children can use your device without inadvertently changing any settings, making calls or accessing inappropriate content. The module consists of **Children's corner**, a restricted environment to control app usage, and **Kids' Browser**, a child-safe browser app.



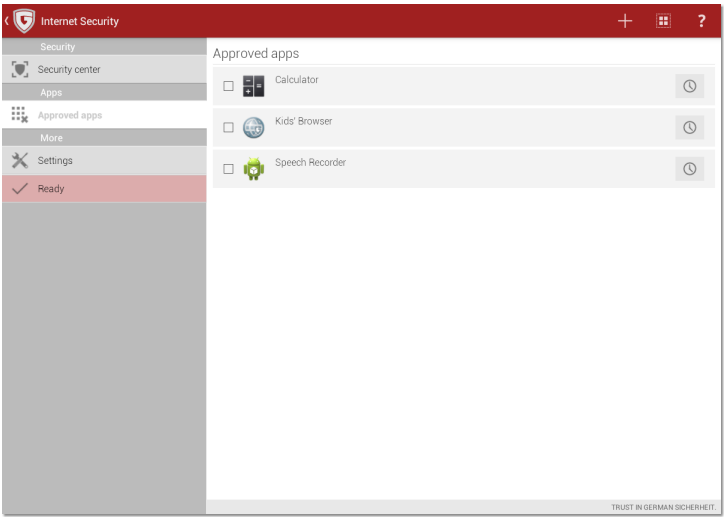
4.3.1. Children's corner

The dedicated **Children's corner** functions as a restricted environment in which only previously approved apps can be run. From the **Parental controls** screen, you can add apps to the **Children's corner** by tapping the settings symbol. **Approved apps** lists all apps that can be used in the **Children's corner** environment. Tap the + symbol in the top right corner to add apps to the list. By default, approved apps can be used for an indefinite amount of time. To configure a time limit, tap the clock symbol and choose a period of time between 15 minutes and 4 hours. To remove one or more apps from the list, select them and choose **Done** in the top left corner.

The **Settings** panel allows additional configuration:

- **Enable flight mode**: Activate flight mode, which disables mobile network and WLAN connectivity.

- **Switch off WiFi**: Disconnect all wireless networks and disable WLAN connectivity.
- **Block incoming calls**: Block incoming calls. Outgoing calls can be placed, if a telephone app has been approved.
- **Permit emergency call numbers**: The telephone app can be used for emergency calls only. All other numbers will be blocked.
- **Set volume**: Ignore any volume changes.



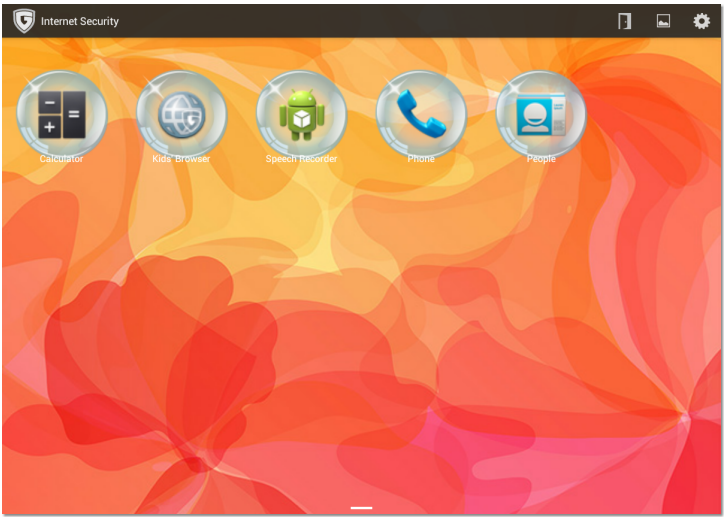
After configuring approved apps and settings, tap the **Ready** button on the left side of the screen to return to the **Parental controls** screen.

> **Children's corner** carries out app protection using its strict whitelist-based settings. Previously configured settings for **Protected apps** are ignored. **Calls / SMS** filters are inactive. To allow telephone usage, the Telephone app can be added to the **Approved apps** list, optionally permitting only emergency calls.

Children's corner can be launched by tapping the power symbol on the right side of the screen. It features a desktop with shortcuts to the previously approved apps. All other apps will be blocked. The exit symbol is protected with a password (identical to the one used for **SMS commands**/**Protected apps**). To prevent the Android home button from being used to reach the default Android home screen, G DATA INTERNET SECURITY FOR ANDROID should be configured as the default launcher. The first time the home button is used, you will be offered the possibility to do so.

The desktop background image can be changed by tapping the background symbol in the top right corner. By tapping the settings symbol, the desktop layout can be configured:

- **Rows in landscape**: Change the number of icon rows in landscape mode (between 4 and 8).
- **Columns in landscape**: Change the number of icon columns in landscape mode (between 2 and 5).
- **Rows in portrait**: Change the number of icon rows in portrait mode (between 2 and 5).
- **Columns in portrait**: Change the number of icon columns in portrait mode (between 4 and 8).
- **Icon size**: Change the size of app icons.
- **Background**: Change the background image of app icons.
- **Background size**: Change the size of the app icon background images.
- **Text size**: Change the font size for app names.
- **Text color**: Change the font color for app names.



4.3.2. Kids' Browser

Kids' Browser is a browser app which only allows visits to child-safe websites. Its whitelist is maintained by German consortium FragFinn (**www.fragfinn.de**), a cooperation between the German government, media companies and other partners including G DATA Software AG. In combination with **Children's corner**, Kids' Browser can be used to offer your children controlled access to the internet, making sure they cannot access any questionable content. Kids' Browser is automatically installed as a separate app when you install G DATA INTERNET SECURITY FOR ANDROID.

5. Calls / SMS

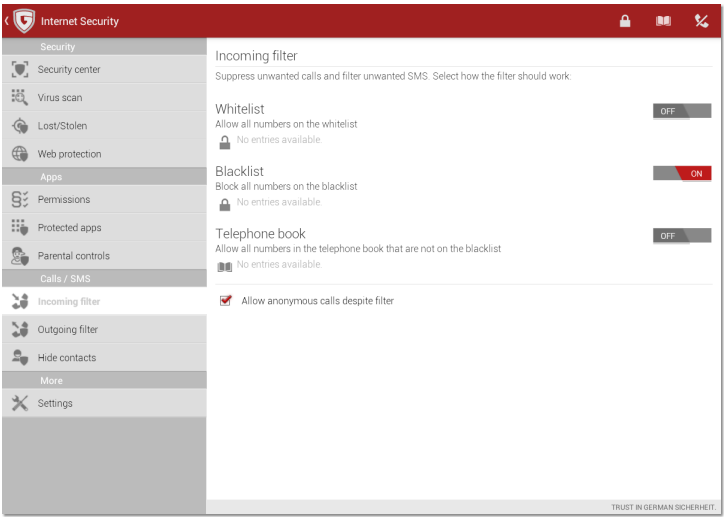
5.1. Incoming filter

The **Incoming filter** filters incoming calls and SMS messages. It can be configured to operate in one of two modes:

- **Whitelist**: Allow incoming calls and SMS messages from phone numbers on the whitelist.
- **Blacklist**: Allow all incoming calls and SMS messages, except from phone numbers on the blacklist.

Enable the **Telephone book** option to allow all numbers in the telephone book, regardless of white- or blacklist. Calls from unknown numbers can be allowed or blocked by ticking or unticking the checkbox **Allow anonymous calls despite filter**. For a log of suppressed calls and SMS messages, tap the phone symbol in the top right corner.

To view and edit the black- or whitelist, tap the respective lock symbol. To add a number to the list, tap the + symbol. Phone numbers can be added from the address book, from the call history and by manually entering them.

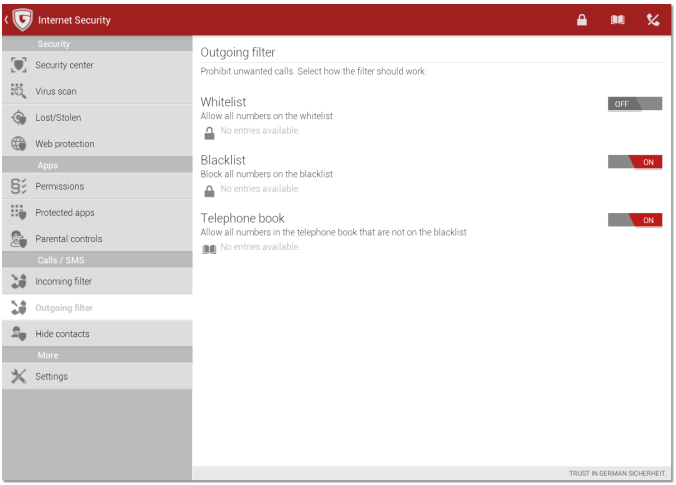


When entering a phone number manually, you can use wild cards to match multiple numbers at once. Asterisks match multiple characters, periods one. For example, entering *0180** will match all phone numbers starting with 0180. Entering *012 345678.* will match phone numbers 012 3456780 through 012 3456789, but not 012 34567800. National and international number formatting are evaluated independently. For example, for an incoming or outgoing call with number 012 3456789, the

international format 0049 12 3456789 is evaluated against the wildcard as well. It counts as a match when either or both of the formats match the wildcard.

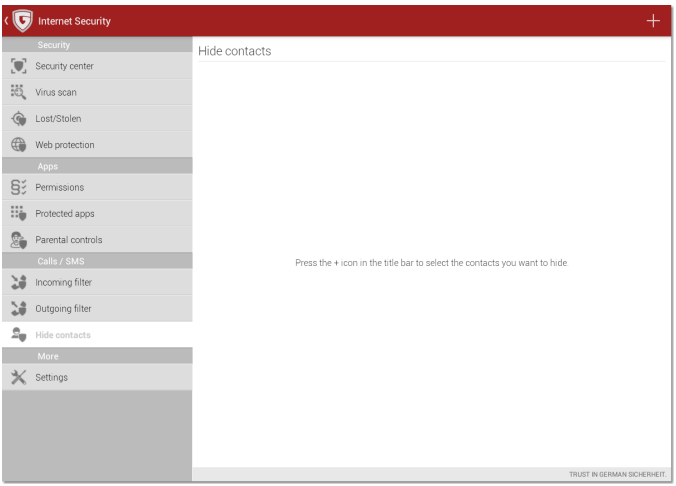
5.2. Outgoing filter

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



5.3. Hide contacts

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



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

6. Settings

6.1. General

The **General** section includes tray icon and scan log settings.

- **Tray icon**: Displays the G DATA INTERNET SECURITY FOR ANDROID icon in the app tray.
- **Save logs**: Saves scan logs to be viewed in the **Security center**.

6.2. Virus scan

The section **Virus scan** lets you configure automatic and scheduled virus scans.

- **When installing apps**: Enable an automatic virus scan for newly installed applications.
- **Periodically**: Enable the scheduled virus scan.
- **Battery save mode**: Postpone the scheduled virus scan if the device is in battery save mode.
- **Only while recharging**: Run the scheduled virus scan only when the device is being charged.
- **Interval**: Specify the interval of the scheduled virus scan.
- **Type**: Scheduled virus scans will scan only **Installed applications** or the **System (full scan)**.

6.3. Update

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

- **Automatic update**: Automatically check for software and virus signatures. If this option is disabled, you can still initiate a manual update.
- **Update frequency**: Set an update interval (in days).

- **Only via WLAN**: Updates are only downloaded automatically when there is WLAN connectivity.
- **Server region**: Select the update server. Upon the first check for updates, the nearest update server is automatically selected.
- **Access data & subscriptions**: Register G DATA INTERNET SECURITY FOR ANDROID using your license key. If you have already registered before, enter your user name and password.

6.4. Web protection

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

- **Only via WLAN**: Only scan websites when there is WLAN connectivity. This helps minimize data traffic when using a mobile data network but increases browsing risks.