Modul Android-Einstellungen

Module Android settings

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

Android settings - General

Settings

Password: Under Change Password, set a general password for all Android clients. The password must consist of four to five digits that are not consecutive (e.g. 1452; 14789; 11310).

The password can be set separately for each client.

Updates

The Updates section covers settings related to updates.

- **Automatically**: You can configure whether the Android client should automatically check for software and virus signatures. If updates are not downloaded automatically, the user can still initiate a manual update. If you choose automatic updates, you can set the **Interval** and limit the updates to happen only when there is Wi-Fi connectivity.

Web protection

The Web protection blocks phishing websites from being opened in the Android browser and in Chrome. Since some data traffic is required to check the list of phishing websites, web protection can be configured to only look up websites when there is Wi-Fi connectivity. The Web protection section therefore includes the possibility to limit web protection to wireless networks.

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

Virus check

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

- **When installing apps**: Enable an automatic virus check for newly installed applications.
- **Periodically**: Enable a periodic virus check. Tick the checkbox Periodically and specify the Interval.
- **Power save mode**: Postpone the periodic virus check if the device is in power save mode.
- **Only while recharging**: Run the periodic virus check only when the device is being charged.
- **Type**: Scan System (full scan) or only Installed applications.

Synchronization

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

Android settings - Policies

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

General settings

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

- **Corporate**: G DATA Internet Security for Android will use settings from the corporate profile, which is regularly synchronized with G DATA ManagementServer. The user is not allowed access to any settings. This is the recommended setting for corporate devices.
- **Private**: G DATA Internet Security for Android will use settings from the private profile, which is not synchronized with G DATA ManagementServer. The user is allowed access to all settings in G DATA Internet Security for Android.
- **Mixed**: The user can freely switch between the corporate and private profiles.

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

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

- **Allow camera access**: Allow access to the device's camera (Android 4.0 and higher).
- **Encryption required**: Require full device encryption to be enabled (Android 3.0 and higher).
- **Allow rooted devices**: Allow devices that have been rooted. If disabled, rooted devices are blocked using the remote maintenance password defined under **Lost/Stolen**. If disabled, rooted devices cannot access the wireless network defined under **Allow WLAN access if requirements are met**.

Allow WLAN access if requirements are met

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

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

Android settings - Lost or stolen

The Lost/Stolen tab offers a range of functions that help protect devices and their data if they go missing. Devices that are stolen or lost can be remotely locked, wiped, located or muted by sending an SMS from a trusted phone number. Using Firebase Cloud Messaging, these anti-theft functions can also be triggered manually at any time.

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

SMS commands

This function is only available until version 14.3.0 due to changed andoid guidelines.

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

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

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

Theft detection

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

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

Emergency action

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

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

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

Android settings - Apps

The Apps panel lets you configure access to apps on managed devices. To block or allow apps, first decide whether the filter should work in Blacklist or Whitelist Mode. In Blacklist mode, all apps on the blacklist will be blocked or password protected; all others will be accessible. In Whitelist mode, all apps on the list will be allowed or password protected; all others will be blocked. The Password (a PIN code) is used to access blocked apps. You can also choose to enter a Recovery email address to which the password will be sent in case you forget it.

Under **Available apps**, all apps that have been installed on the currently selected device(s) are listed. For each app, you can see its **Name**, **Version** and **Size**. Using the arrow controls apps can be moved to the white-/blacklist. For apps on the white-/blacklist, you can enabled or disable **Password protection**.

Android settings - Phone book

This function is only available until version 14.3.0 due to changed andoid guidelines.

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

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

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

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

Android settings - Calls and SMS

This function is only available until version 14.3.0 due to changed andoid guidelines.

Incoming calls/SMS

Under Incoming calls/SMS, you can define how Internet Security should treat incoming communication. Uncheck **Allow anonymous calls despite filter** to block all anonymous incoming calls. Enabling the additional option **Add phone book to the filter entries** will allow contacts with an entry in the Android or Internet Security phone books through the filter, in addition to any whitelisted contacts.

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

Outgoing calls

Under Outgoing calls, you can define how Internet Security should treat outgoing phone calls. Enabling the additional option **Add phone book to the filter entries** will allow contacts with an entry in the Android or Internet Security phone books to be contacted, in addition to any whitelisted contacts.

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

If an attempt is made to call a blocked contact, the user will be informed and offered the possibility to request the contact to be permitted. The permission request will be added to the **Security events** module. It can be used by the administrator to directly add a blacklist or whitelist exception for the contact.