TRUST IN GERMAN SICHERHEIT

G DATA TechPaper #0273

Mobile Device Management

G DATA CyberDefense AG | September 2019

Contents

1. Introduction

Traditionally, enterprise network and system administrators have always managed homogenous groups of client devices. The process of planning and provisioning network clients almost exclusively dealt with desktop computers. This predictability simplified deployment of network infrastructure, client hardware and applications, ensuring uniformity across all network devices. However, since smartphones and tablets have taken the world of consumer electronics by storm, the technology landscape has become a lot more complicated. Trends like the Consumerization of IT and Bring your own device have introduced device diversity to the enterprise. Administrators are left with the task of providing broad access to resources while guaranteeing security. This TechPaper aims to outline trends in the use of smartphones and tablets in enterprise networks (chapter 2) as well as practical management strategies for administrators dealing with increased mobile device usage (chapter 3). Chapter 4 discusses the usage of G DATA Mobile Device Management.

2. Mobile devices in the enterprise

The rate of technology adoption in enterprise environments is significantly slower than the rate at which consumers embrace new devices. Even if a product can be easily incorporated in workflows, it has to be tested for compatibility issues with the corporate infrastructure – a process which can be very budget- and time-demanding. Ever since Apple popularized the mobile device category with the iPhone and iPad product launches, hundreds of millions of home and corporate users alike have gotten hooked on the combination of advanced technology and ease-of-use. However, many corporations are still struggling to properly integrate these devices into the enterprise environment. This delay in adoption often leads to tension between end users' expectations and the functionality that currently deployed enterprise solutions can offer. Two major trends in enterprise IT cover illustrate this conundrum: Consumerization of IT and Bring your own device (BYOD).

Dubbed Consumerization of IT, the influence of privately used consumer devices on enterprise IT solutions has grown immensely. End users have gotten used to permanently available mobile internet, cloud-based messaging and e-mail, as well as huge quantities of apps to customize the mobile experience. Although no administrator would deny that the use of these services can be very convenient, some of the advantages are inherently at odds with enterprise IT structures. The rate at which new apps are released for mobile platforms far exceeds the capabilities of administrators to test individual apps for compatibility and security. The use of cloud services often means storing data on servers that are managed by third parties. Even though end users have come to expect such services from their devices, not all enterprises are technically ready to offer them in a way which meets IT policies.

Even when mobile devices and services are not being actively deployed in an enterprise environment, that does not mean administrators do not encounter them at all. This trend is called Bring Your Own Device (BYOD): end users bring their own devices to work and expect to be able to use company infrastructure, such as Wi-Fi access and network shares. Similarly, many e-mail server configurations allow remote access using mobile devices, regardless of whether that device is managed or not. BYOD often leads to knee-jerk reactions: to make sure that no sensitive data is leaked or malicious software

enters the network, mobile devices are blocked from the enterprise infrastructure altogether or device functionality is severely limited by oppressive policies.

However disruptive it may sound, it is important to realize that enterprise mobile device usage is not a black-or-white phenomenon. BYOD and Consumerization of IT may seem to destabilize a perfectly organized environment, but there are several benefits to deploying corporate devices or managing private ones. Using a device management solution can help take advantage of the positive sides of mobile device usage while limiting its effects on the rest of the enterprise infrastructure.

2.1. Benefits

The integration of smartphones and tablets in enterprise workflows has obvious advantages, regardless of whether they are centrally deployed or brought in by employees. Offering mobile access to enterprise resources can greatly improve productivity for remote workers and contractors. A combination of access controls and device management enables safe and effective use of their device to access company resources while outside the office. Traveling no longer means a lack of communication: employees can remotely keep track of e-mail, calendar and notifications.

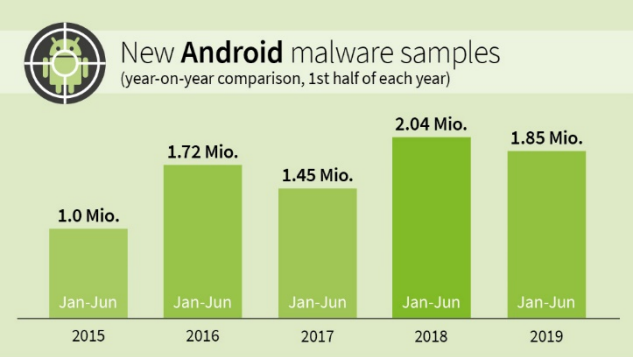
Enterprise devices and applications often have a higher barrier to entry with regards to usability, whereas consumer technology has often been engineered to provide a level of familiarity to end users. This reduces the learning curve for employees, allowing them to quickly get used to company issued devices.

Finally, in a BYOD environment, enterprises save money by not having to heavily invest in device deployment. Instead of buying and deploying new smartphones and tablets, employee devices can be provisioned with device management software and directly used for corporate purposes. Companies are also no longer responsible for replacement devices in case an employee loses or breaks a smartphone or tablet.

2.2. Risks

Even though mobile device adoption can have many positive effects on enterprise productivity, there are some challenges. Mobile devices are consistently perceived as the weakest link of enterprise infrastructure (CyberEdge 2017 Cyberthreat Defense Report). As with PCs, mobile devices are susceptible to malware. Especially Android and iOS are at risk: with a combined market share of 99.1 percent (Gartner), they are a prime target for criminals. In the 1st half of 2019, G DATA security experts investigated over 1.85 million new Android malware samples. Android malware is used for a variety of nefarious purposes, including:

- Stealing data, such as e-mails, login data and sensitive documents.
- Causing excessive costs by sending SMS messages to (foreign) premium phone numbers
- Spying on mobile banking apps
- Locking devices in order to extract a ransom (ransomware)



However, malware is not the only threat to mobile devices. When browsing the internet, phishing websites may try to convince the user to enter personal data into a seemingly innocuous form. And even if the device itself is safe, that does not mean it can be safely used within corporate contexts. When employees use mobile devices to access corporate documents, it needs to be made sure that sensitive information does not leak, either by accident (for example: by uploading it to a file-sharing service) or on purpose (insider threat).

In addition to security risks, mobile devices may also cause a productivity hit. The use of apps should be restricted to make sure that employees do not spend an excessive amount of time on games or other pastimes. Contact management can help lock down use of the telephone functionality to the absolutely necessary, saving time and costs.

The benefits of mobile device usage in the enterprise outweigh the risks. However, the latter still need to be mitigated. An integrated mobile device management policy can help manage security risks as well as productivity issues and ensures safe and efficient use of smartphones and tablets.

3. Mobile device management

As an administrator, ignoring consumerization and BYOD is near impossible. End users will continue to demand enterprise smartphones and tablets that adhere to the usability paradigm they have gotten used to. If such devices are not being actively deployed, they will bring their own. Considering the advantages mobile devices can bring to productivity, the goal of mobile device management should be to maximize productivity while guaranteeing security and minimizing costs.

3.1. Deployment and administration

Before smartphones or tablets can be managed by a mobile device management solution, they have to be deployed. Deployment involves a one-time initial connection between device and server, after which the device will periodically report back to the server and can be remotely managed. Communication between server and device takes place in the form of internet traffic (when a direct connection to the server can be established), push messages (often based on vendor-specific cloud messaging solutions) or SMS messages (when no mobile internet connection is available). A permanent connection between device and server is not required: the device can carry out server policies even if there is no contact to the server. This means that devices are protected at all times, even outside the enterprise environment.

Deployment should be streamlined as much as possible. New, company-managed devices should always be equipped with mobile device management features before being handed over to employees. BYOD devices should be denied access to the corporate network and its resources until they have been equipped with mobile device management. Optionally, a guest network can be used for devices that do not meet the requirements or are used by visitors.

To avoid an increased workload, administrators should choose a device management solution that integrates with existing management structures. The use of multiple back-ends should be avoided. Ideally, mobile devices can be managed using the same kind of interface and reporting capabilities that are available for other device types in the network, in order to support an integrated workflow and consistent configuration.

For BYOD devices, the legal aspect of device management should be considered. Because this type of devices is not company property, administrators do not automatically have the right to manage it. Especially permissions like remote wipe can be controversial. Depending on the legal situation, companies may have to ask permission from the end user before enrolling a device in mobile device management. It is recommended to define an end user license agreement (EULA) that explains the actions that the company needs to be able to execute on the device. The end user can either accept or decline the agreement, but access to corporate resources will not be available if the EULA is declined. Even for non-BYOD devices, a EULA can be useful.

3.2. Anti-theft

Mobile devices increase risk levels for the physical infrastructure and information-based workflows. Between employees bringing sensitive files with them on the road and mobile devices getting lost or stolen, it is easier than ever to accidentally leak confidential information. To make sure that corporate e-mails, documents and other communication cannot be accessed when a device is lost or stolen, several measures can be defined. Firstly, it can be helpful to try to recover the device. Locating it using GPS technology or triggering an alarm sound can help. If locating the device is not an option or does not yield any usable results, locking it will make the device useless. As a last measure, devices can be reset to the factory defaults, wiping all data on the device.

3.3. Apps

Part of the charm of mobile devices is the fact that their default functionality can be expanded by installing apps. Even in a corporate context, this can be extremely useful: productivity tools or configuration apps can significantly increase the amount of use cases for mobile devices. At the same time, corporate devices should provide a controlled environment, making sure that apps cannot cause compatibility problems, leak sensitive information, or spread malware. App management is a powerful way to control the functionality of a mobile device, balancing security with usability.

Separating the good apps from the bad can be a difficult task. Some apps are clearly unsuitable for corporate environments, such as games. Others may serve some purpose, but can possibly harbor privacy risks, such as online file storage services. Even apps that seem risk-free may later turn out to be compromised, either because the app itself contains security flaws, because its backend services are compromised, or because it insecurely transmits information. Productivity is also a factor: for example, employees that only need a smartphone in order to call and make appointments, would only get access to phone and calendar components, while employees that are working on documents on the road get access to browser, office apps and other required components.

3.4. Real-time and on demand protection

Like desktop and laptop clients, mobile clients are also vulnerable to online attacks. Rooted Android devices in particular do not have sufficient protection mechanisms against malicious apps from unknown sources, but even malevolent apps that manage to sneak their way into the official app stores can have severe implications. Similarly, websites may try to serve malware, take advantage of vulnerabilities in the operating system or otherwise deceive the end user. As on desktop computers, phishing websites may try to coax users into handing over passwords or other sensitive data. To counter these threats, protection measures should be configured for all managed mobile devices.

Real-time protection protects devices all the time without requiring user interaction. This includes technologies like phishing protection and automatic virus scan. On demand protection, on the other hand, is only activated once an end user or administrator triggers it. For example, a virus scan can be manually initiated to make sure that no malicious apps have been previously installed on the device.

Real-time and on demand protection solutions differ greatly per client platform. Whereas Android clients are especially susceptible to malicious apps, iOS devices are more vulnerable to data loss or phishing threats. Mobile device management solutions should offer measures to optimally suit each mobile platform: a one size fits all module does not do justice to the wide range of threats that devices face.

3.5. Contact management and filtering

For devices that are used in a corporate context, controlling communication streams can be essential. Blocking apps can help if communication should be entirely prevented, but in some scenarios a more fine-grained filter should be deployed. Rather than completely blocking the Phone app if a device is only meant to be used for work-related communication, outgoing and incoming calls could be filtered if they do not meet corporate criteria. For example, a company that supplies its employees with phones to communicate with headquarters while on the road could block all phone calls except those with pre-approved corporate contacts.

Central to contact management is a managed phone book. Contacts stored on the device can be synchronized to the central server and administrators can push the latest phone numbers to devices. Like app management, contact management can be used for individual devices, but is best combined with group-based management. Individual phone numbers can be allowed or blocked for groups of devices at once or a complete corporate phone book can be pushed to all devices.

4. Using G DATA Mobile Device Management

G DATA offers a mobile device management module as part of its business solutions. G DATA Antivirus Business, G DATA Client Security Business, G DATA Endpoint Protection Business and G DATA Managed Endpoint Security all include the Mobile Device Management component with iOS and Android support. It is fully integrated with other parts of the business solutions and can be managed from the same application (G DATA Administrator). This is a clear advantage compared to standalone solutions, which require separate administration and often have a steep learning curve.

4.1. Android

G DATA Mobile Device Management for Android is powered by G DATA Mobile Internet Security. The functionality of the app is centrally managed through G DATA Administrator and offers a full suite of security and productivity features for all devices with Android 4.0 or newer.

4.1.1. Deployment and administration

The first step is to deploy G DATA Mobile Internet Security to all Android devices. To make sure that only authorized network clients can connect to the server, a password needs to be defined server-side before deploying any clients. The same password will have to be entered in the app afterwards to allow it to authenticate with G DATA Management Server. Client installations are initiated using G DATA Administrator. The deployment process is carried out via e-mail. An activation e-mail containing a link to the installation file can be sent to one or more e-mail addresses. After downloading the file on the Android client and confirming its requested permissions, G DATA Mobile Internet Security will be installed and can be started from the Android app menu. Deployment is completed by connecting the Android app with Management Server, after which it will connect to the server and immediately download the default mobile device management configuration.

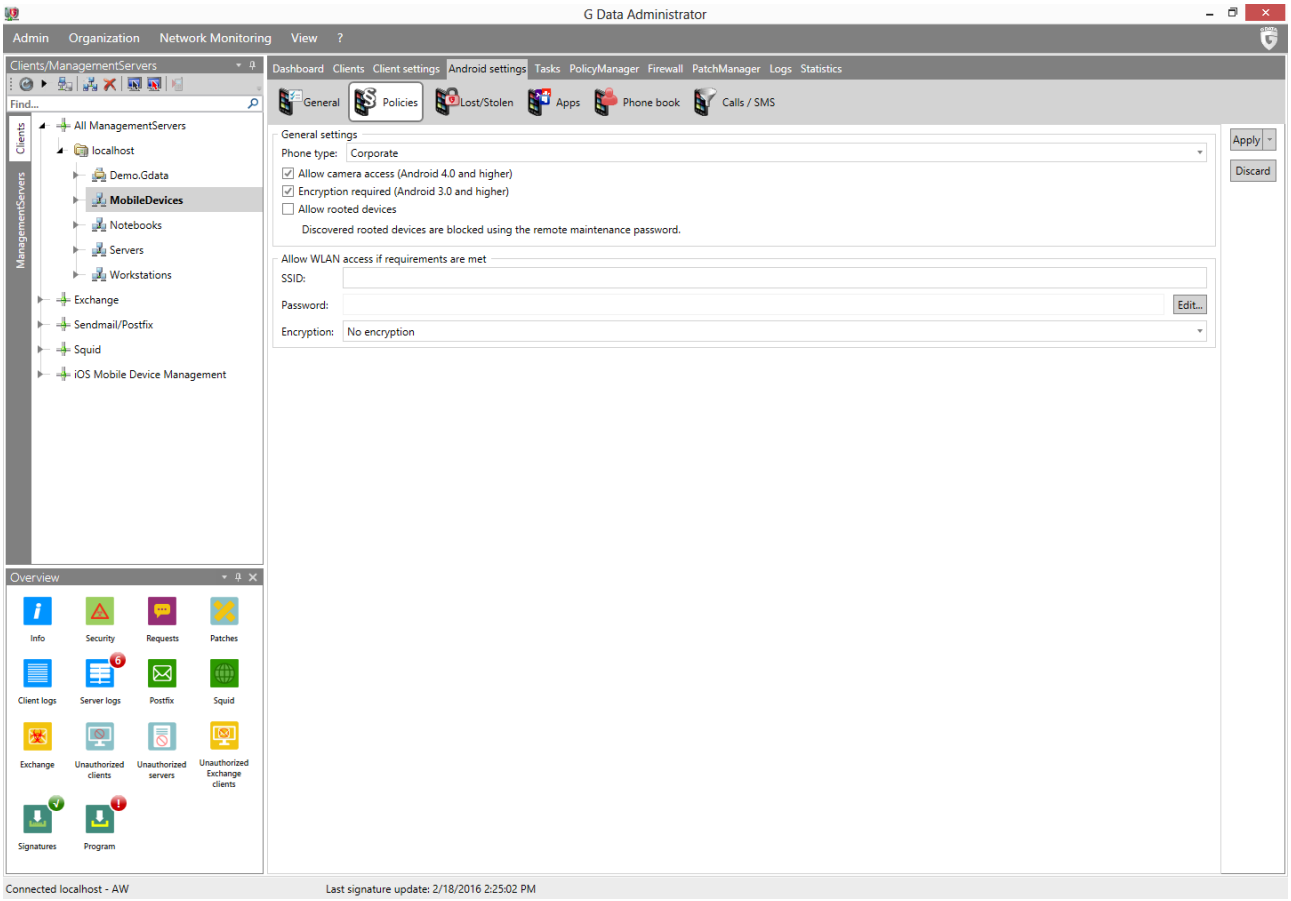


Image 1: G DATA Administrator, Android settings, Policies

As soon as it has connected to Management Server, the device will automatically show up in G DATA Administrator. Because Android devices show up as clients in the regular client list, they can be moved to

groups. Creating a dedicated group is recommended, with subgroups for the various device access types (corporate, private or mixed), for the various departments that are using Android devices, or any other division. This allows for efficient administration and lets the device automatically inherit the correct settings.

For each device or group, a phone type can be defined under ANDROID SETTINGS > POLICIES. For devices that have been issued by the company and are only meant for company use, the phone type CORPORATE is recommended. This will lock down the client-side setting menus of Mobile Internet Security, so that users cannot inadvertently change remotely managed settings while connected to the corporate network. Phone type PRIVATE can be used for devices that have not been issued by the company. This allows the end user full access to the settings of Mobile Internet Security. Phone type MIXED serves company-issued devices that are used for corporate as well as private communication.

Some basic settings should be configured directly after deploying a new device. Update schedule and synchronization settings should always be defined. Both settings depend on the usage pattern for the device. Devices that often connect to a wireless network (Wi-Fi) can be configured to update their virus signatures automatically and synchronize data with the Management Server every few hours. Devices that are mostly used outside the company network, or connect to the internet using a mobile data plan, can be configured to update less often, or manually, or only when connected via Wi-Fi. The same applies to synchronization: different settings can be configured for Wi-Fi and mobile data plans. If required, devices can be assigned an End User License Agreement. Legal obligations may require companies to inform end users that their device can be remotely managed.

4.1.2. Anti-theft

Anti-theft measures can be triggered automatically as well as manually. Some can be configured to be executed if something happens to the device (like a SIM card change). Others can be triggered using G DATA Administrator to send a command via Google Firebase Cloud Messaging. Finally, commands can be sent by SMS.

To enable all measures, several settings have to be configured under ANDROID SETTINGS > ANTI-THEFT. To use SMS commands, a remote maintenance password (a numerical PIN code) should be entered. It will also function as a lock screen password if that has not been explicitly defined. A trusted phone number needs to be set to make sure that the remote maintenance password reset command cannot be sent by anyone – only a password reset sent from the trusted phone number will be executed. Finally, an e-mail address should be entered to receive feedback from actions that provide it.

When a device gets lost or stolen, the quickest method of executing an action on it is sending an SMS message to it. Administrators can individually select commands that can be sent to the device. The following measures are available:

- Send the administrator an e-mail with location data.
- Reset device to factory defaults. All personal data will be wiped.
- Trigger alarm sound.
- Mute all ringtones, except the one triggered by the alarm sound option.
- Enable lock screen using the lock screen password.

- Set lock screen password.

If a device is stolen, its SIM card is often removed to prevent the original owner from contacting the device via its phone number. This means SMS messages will not be delivered to the device. As a countermeasure, you can define actions to be taken automatically when the SIM card is changed. The phone's lock screen can be enabled, making the device inaccessible, and the device can be located. In addition to SIM- and SMS-based measures, several actions can also be initiated via G DATA Administrator. The device does not need to be connected to the Management Server network for this to work: it relies on Google Firebase Cloud Messaging, an online service from Google which lets you send commands to Android devices. This requires a Google Firebase Cloud Messaging account, which can be registered for free with Google at https://firebase.google.com.

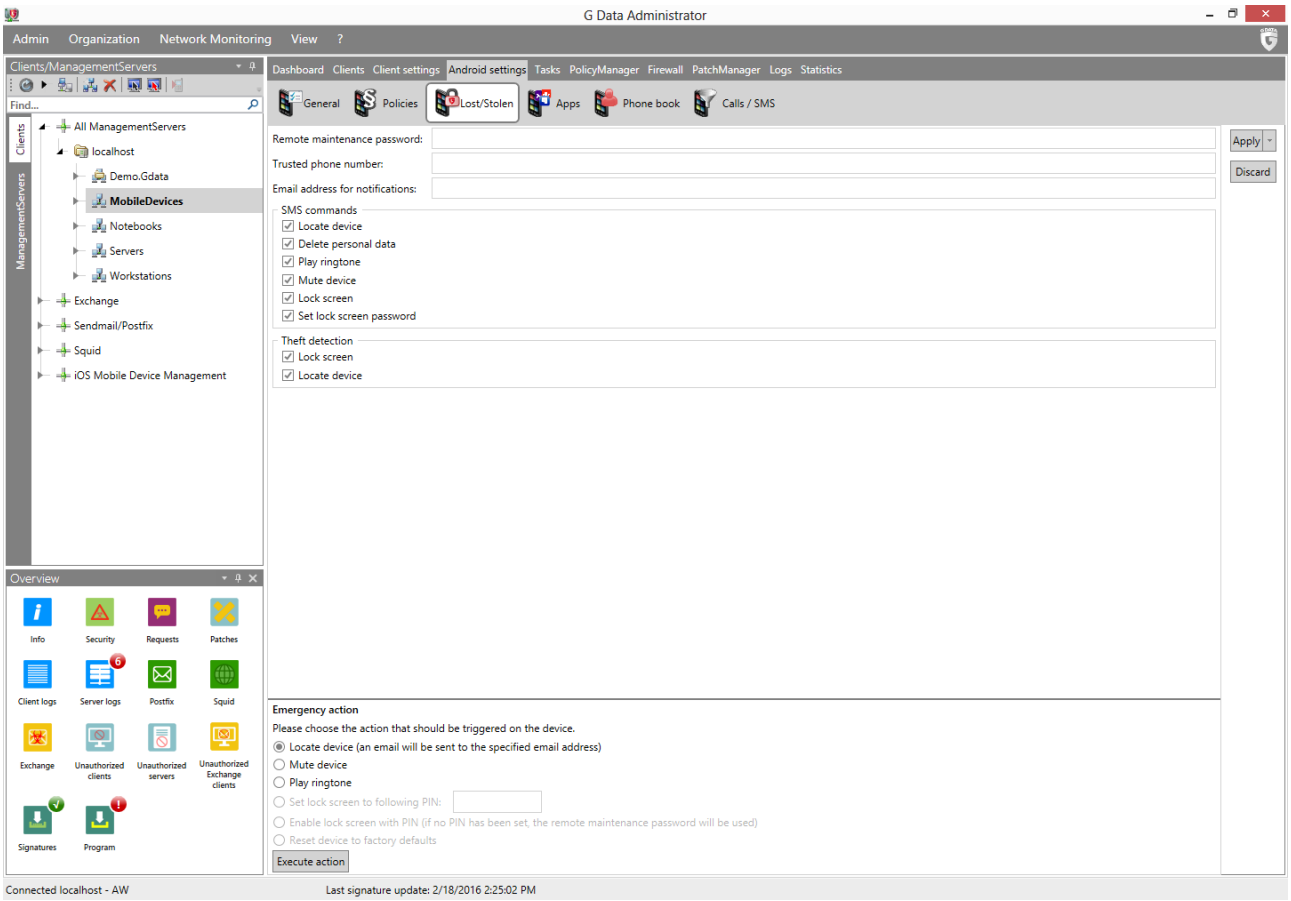


Image 2: G DATA Administrator, Android settings, Lost/Stolen

Because the anti-theft actions can severely affect the usability of the phone (e.g. by removing data from it), it is recommended that the end user is informed by deploying a EULA.

4.1.3. Apps

G DATA Mobile Device Management for Android offers elaborate app management possibilities. As a first step, it can be used to take an inventory of apps that are in use of mobile devices in the network. Each installed app is listed with its name, version and size. For each app, administrators should obtain information about its vendor, its functions and its version history, insofar information sources are

available. For many apps, the official app store(s) will provide enough details, for others it may be necessary to look up the vendor's homepage. Based on this information and on the intended use of the device (based on the device group and type and the network zone), apps can be added to the whitelist or blacklist. This will allow respectively block the listed apps. Using the defined password, apps are blocked from running.

Whether to use a blacklist or whitelist approach depends to which extent the device should be locked down. When app management is used in blacklist mode, it can easily be configured for multipurpose devices on which the end user should be able to install new apps without having prior approval. The risk lies in the fact that essentially all apps can be installed and run. Only after an administrator manually blocks them, will users be prohibited access. A safer but more restrictive method is whitelisting: not a single app can be used unless it has been added to the whitelist. This is particularly useful in cases where a device is configured for a single use. Administrators can then preinstall the required apps, whitelist them, and refuse access to all others.

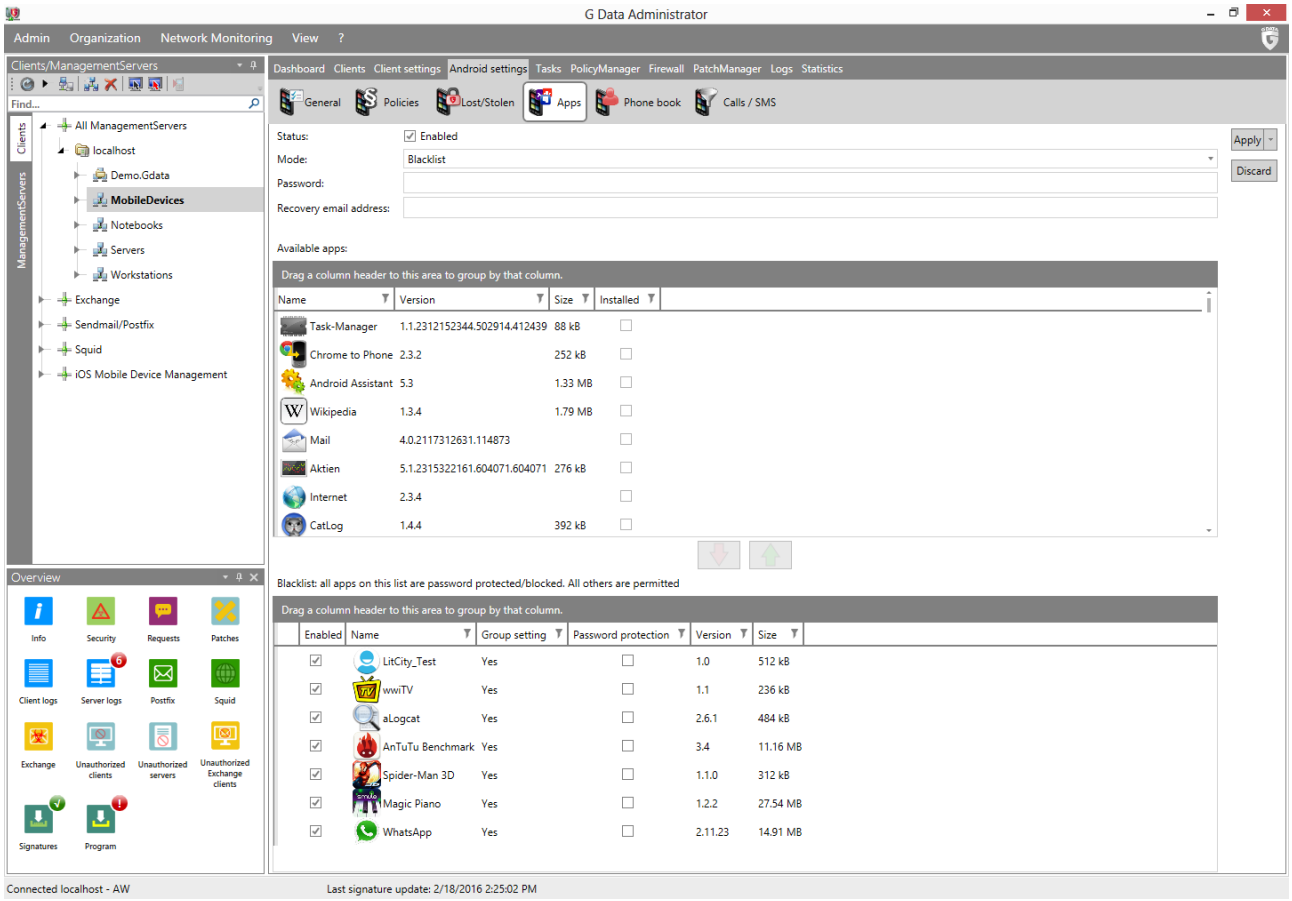


Image 3: G DATA Administrator, Android settings, Apps

If the goal is to only block a few known bad apps, while allowing the user relative freedom, a blacklist approach will do. At the very least, the Android Settings app and Mobile Internet Security itself should be password-protected. This will prevent the end user from tampering with any settings. Blacklisting the official app store makes sure that no other apps can be installed. To completely control a device's app experience, the whitelist approach is the most reliable option. Whitelisted apps can be used without any limitations, but any other apps are blocked. This is most useful for devices that are configured for

maximum security, or for a single workflow. For example, a device that is only to be used by sales representatives may be run in whitelist mode, allowing only the phone component and the sales database frontend to be used.

4.1.4. Real-time and on demand protection

Real-time malware protection is available through the WEB PROTECTION and VIRUS SCAN modules. In addition, functionality can be restricted via the POLICIES tab of G DATA Administrator.

Web protection provides real time protection when using the Android browser. Because web protection can produce a small amount of data traffic, it can be configured to work only when the device is connected via Wi-Fi. The virus scan transparently checks downloaded apps for malware and blocks the installation if it is found to be malicious.

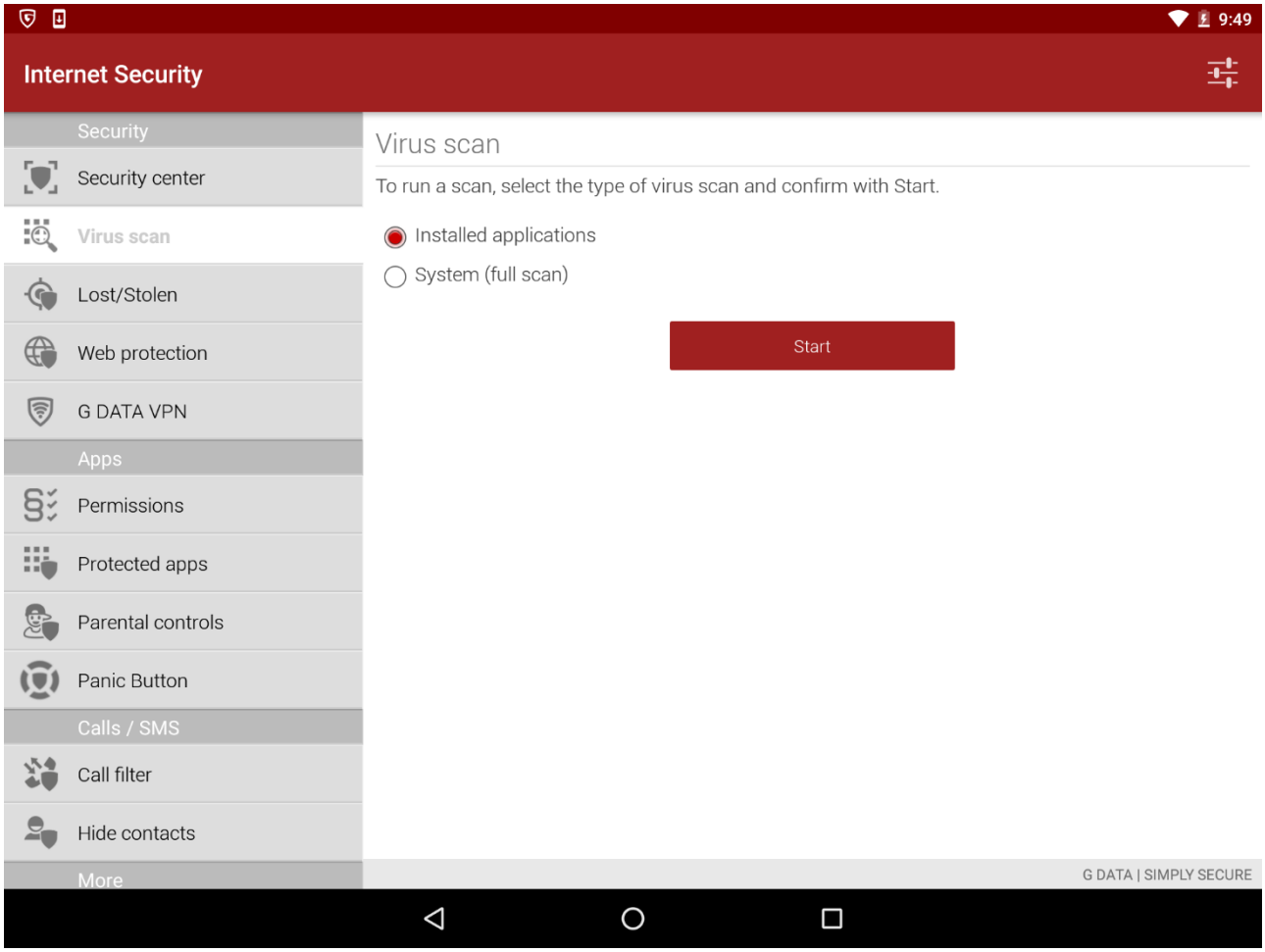


Image 4: G DATA Mobile Internet Security, Security, Virus scan

On demand malware protection is available in the form of a full virus scan for the complete device. A regular scan of all applications is recommended to make sure no malware is lingering on storage media (such as an SD card). Depending on how often the device is used and how often new software is installed or saved on it, the interval can be set to 1 day, 3 days, 7 days, 14 days or 30 days. In most cases, it is recommended to perform a daily check: the scan does not cause any noticeable slowdowns, and

provides maximum security. To make sure that the virus scan is not draining the device battery, it can be configured to only take place while the device is recharging.

On Android devices, the largest threat comes from rooted devices. If the end user has obtained root access to the device, any amount of security on the operating system and app levels can easily be subverted and if malware manages to infect the device, it gains virtually unlimited access to operating system functions. In order to stay in control of managed mobile devices, it is therefore recommended to use the POLICIES tab to refuse network access to rooted devices. In addition, the administrator can enable or disable camera access and/or mandate encryption to protect data stored on the device.

4.1.5. Contact management and filtering

To manage contacts on Android devices, the corporate phone book can be used. Even without using any filtering possibilities, blocking the built-in device phone book and populating Mobile Internet Security's corporate phone book can be an effective way of ensuring control over contact information. Together with the call filter module, it offers extensive contact management and filtering possibilities.

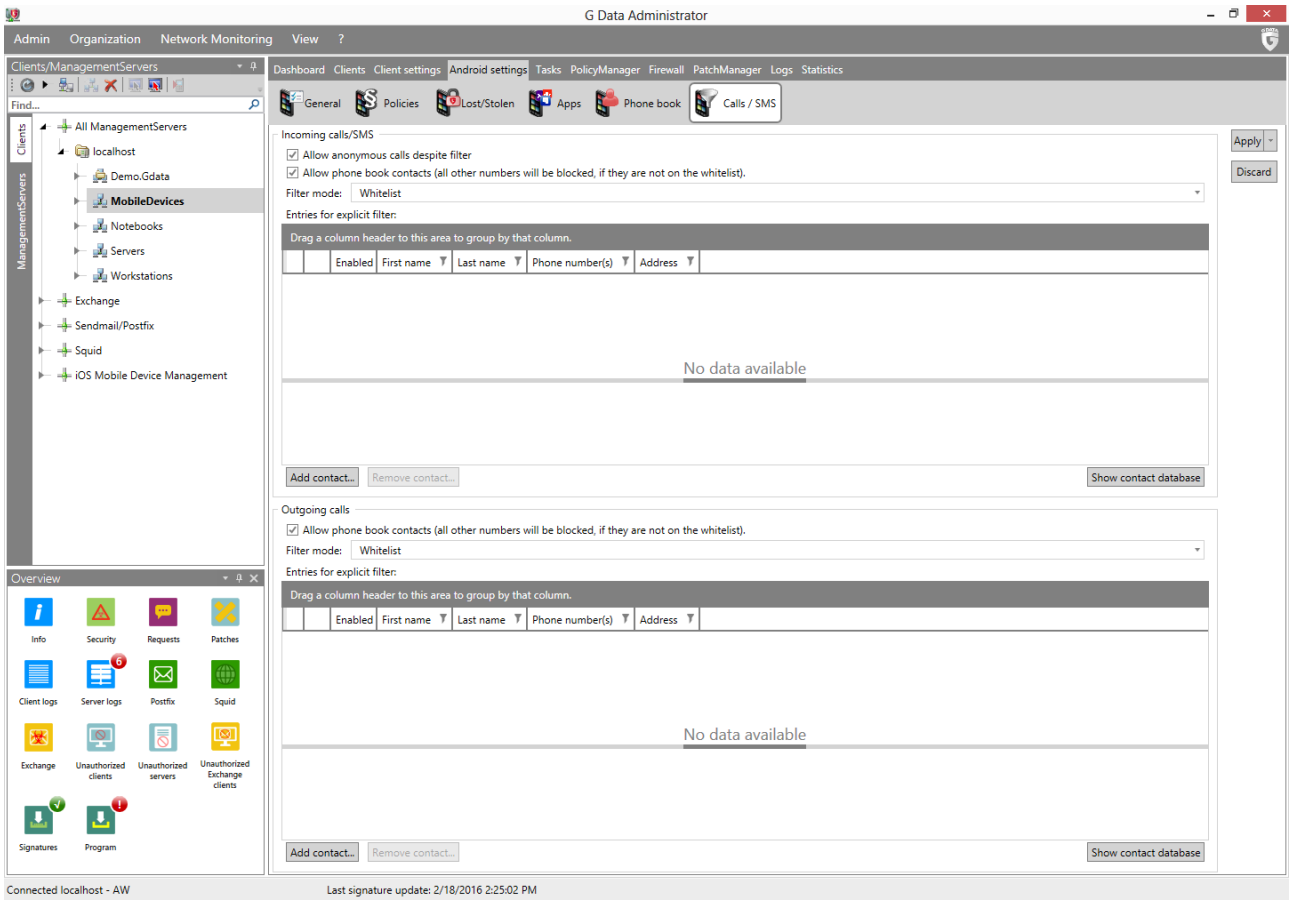


Image 5: G DATA Administrator, Android settings, Calls / SMS

The basis of all functionality is the contact database. It functions as a central hub for all corporate contacts, based on which phone books can be created for various devices, as well as targeted call and SMS filters. For organizations with a limited number of contacts, or for small managed phone books, entering contacts manually is a practical way to quickly populate the contact database. If the network is

using Active Directory, contacts can be imported. With all contacts defined, they can be distributed to the appropriate devices. For example, all devices can be supplied with a complete list of colleagues' direct extensions. Alternatively, combined with a block of the standard phone book app and use of the call filter, groups of devices can be allowed access only to certain explicitly deployed phone numbers in the Phone book.

The call filter can also be used for extensive filtering of incoming and outgoing communication. It functions as a filter on the built-in device phone book. Rather than completely blocking the Android phone book app, the filter allows granular control over communication streams. For example, enabling the whitelist mode, no incoming or outgoing calls will be allowed, except for those numbers that have been added to the whitelist. In blacklist mode, communication is generally allowed, but specific numbers can be blocked.

4.2. iOS

G DATA Mobile Device Management for iOS devices has been designed as an agent-less solution for iOS 7.0 and higher. Using G DATA Administrator, policy profiles can be deployed to one or more iOS devices. This allows administrators to flexibly manage devices while retaining maximum influence over their usage. In order to manage iOS devices, a free account for G DATA Action Center must be created (https://ac.gdata.de). Enter the Action Center user name and password in the ACTION CENTER module of G DATA Administrator in order to enable G DATA Mobile Device Management for iOS.

4.2.1. Deployment and administration

iOS client deployments can be initiated from G DATA Administrator. The deployment process is carried out via e-mail. On the CLIENTS/MANAGEMENTSERVERS > CLIENTS tab, select any node under IOS MOBILE DEVICE MANAGEMENT, click the toolbar button SEND INSTALLATION LINK TO MOBILE CLIENTS and enter a list of e-mail addresses. To customize the appearance of the MDM request on the device, some parameters can be entered. NAME, DESCRIPTION and ORGANIZATION will be displayed in the MDM request as well as afterwards on the GENERAL tab of IOS SETTINGS. The END USER LICENSE AGREEMENT can be used to inform the end user of the fact that the device will be remotely managed.

When the end user opens the link from the installation e-mail on an iOS device, the device immediately shows up in G DATA Administrator (with the SECURITY STATUS on the CLIENTS tab detailing its pending status). As soon as the end user accepts the MDM request, the iOS device can be fully managed through G DATA Administrator.

When an iOS device is selected in G DATA Administrator, a set of iOS MDM modules becomes available. The CLIENTS (IOS) tab shows an overview of all managed iOS devices. For each client, several device-specific properties are displayed, such as its IMEI number, the iOS version and the product name. The SECURITY STATUS column provides warnings for devices without a policy profile as well as MDM installation status alerts. Using the IOS SETTINGS module, administrators can configure anti-theft measures (see chapter 4.2.2) as well as policy profiles (see chapter 4.2.3). The REPORTS (IOS) module can be used to track the status of various push messages, the main method of communication between G DATA Action Center and iOS devices. Reports include profile deployment status and anti-theft function confirmations.

4.2.2. Anti-theft

When a device is lost or stolen, the first action to take is to make sure that no one can access any data on the device. Afterwards, it can be located using GPS (to find and return the device) or the more drastic measure of wiping the device can be carried out (in case there is no chance of finding and returning the device). Apple offers registered iCloud users the Find my iPhone feature. It allows users to log in to a dedicated website and lock, track or erase a device.

As an alternative to the Find my iPhone features, the iOS SETTINGS module lets administrators trigger anti-theft functions on the ANTI-THEFT tab without requiring them to log in to an external website. The device lock and reset functions can be triggered by selecting the respective option and clicking EXECUTE FUNCTION. For devices that have been locked using an unknown passcode, use the option REMOVE PASSCODE.

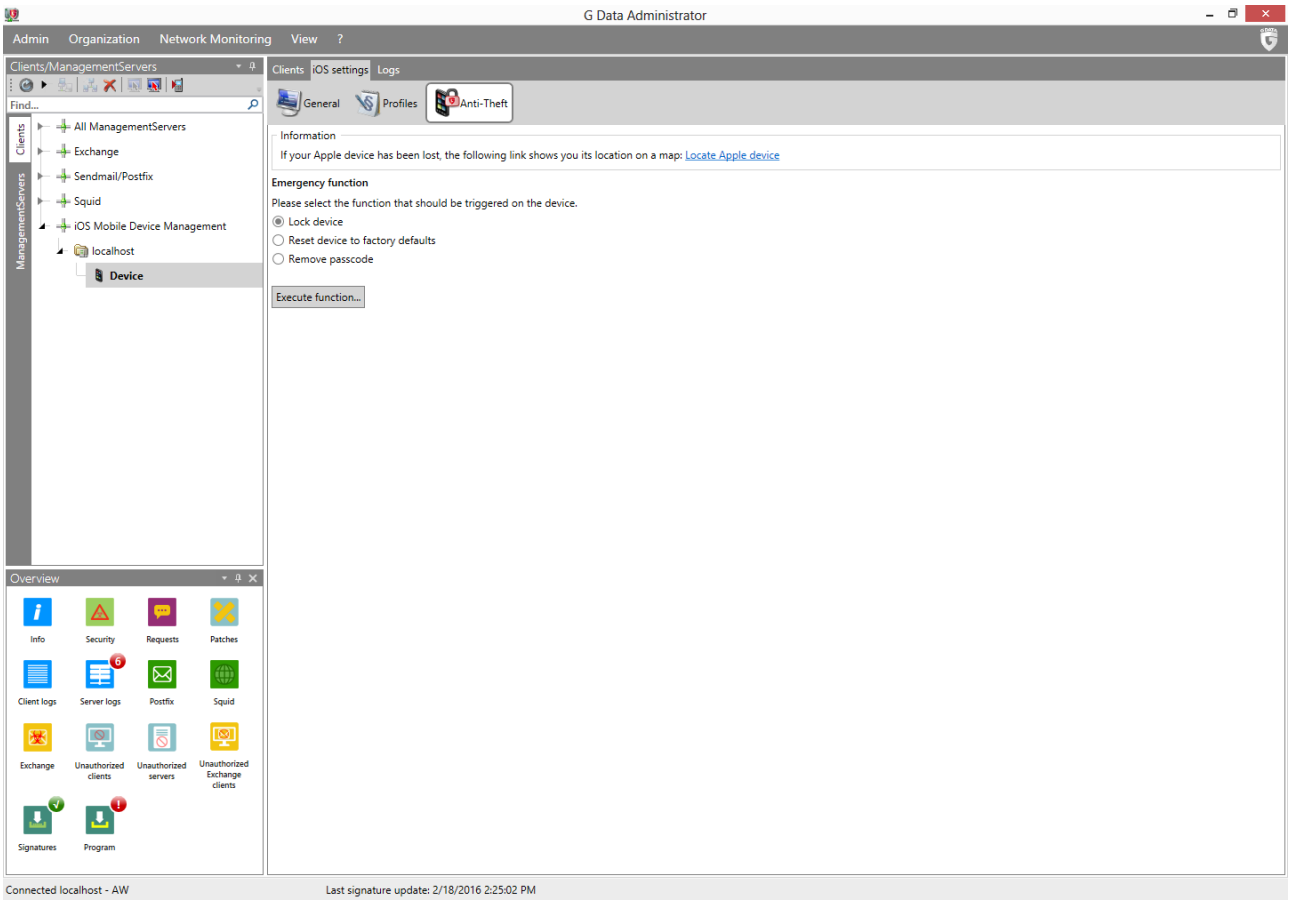


Image 6: G DATA Administrator, iOS settings, Anti-Theft

4.2.3. Apps, protection and contact management

Unlike Android devices, iOS has a unified security management concept, which allows administrators to consolidate security settings covering a wide range of modules into one profile. These profiles can then be applied to multiple devices, reducing the time required to secure all iOS devices in the network.
G DATA Administrator's PROFILES tab can be used to create and edit profiles.

Each profile can contain up to five policies, each of which focuses on a specific type of security settings:

- FUNCTIONALITY RESTRICTIONS: Restrict the usage of iCloud, ensure secure Lock Screen usage, control various other functions.
- PASSCODE SETTINGS: Enforce standards for passcode usage, such as a minimum number of complex characters, a minimum length and a grace period after locking the device.
- APP RESTRICTIONS: Block or allow Safari (including functions such as cookies, pop-ups and JavaScript) and iTunes Store.
- MEDIA CONTENT RESTRICTIONS: Control which media content types are allowed (apps, movies, TV shows).
- WI-FI: Enter Wi-Fi network information, allowing iOS devices to automatically connect to a specific Wi-Fi network.

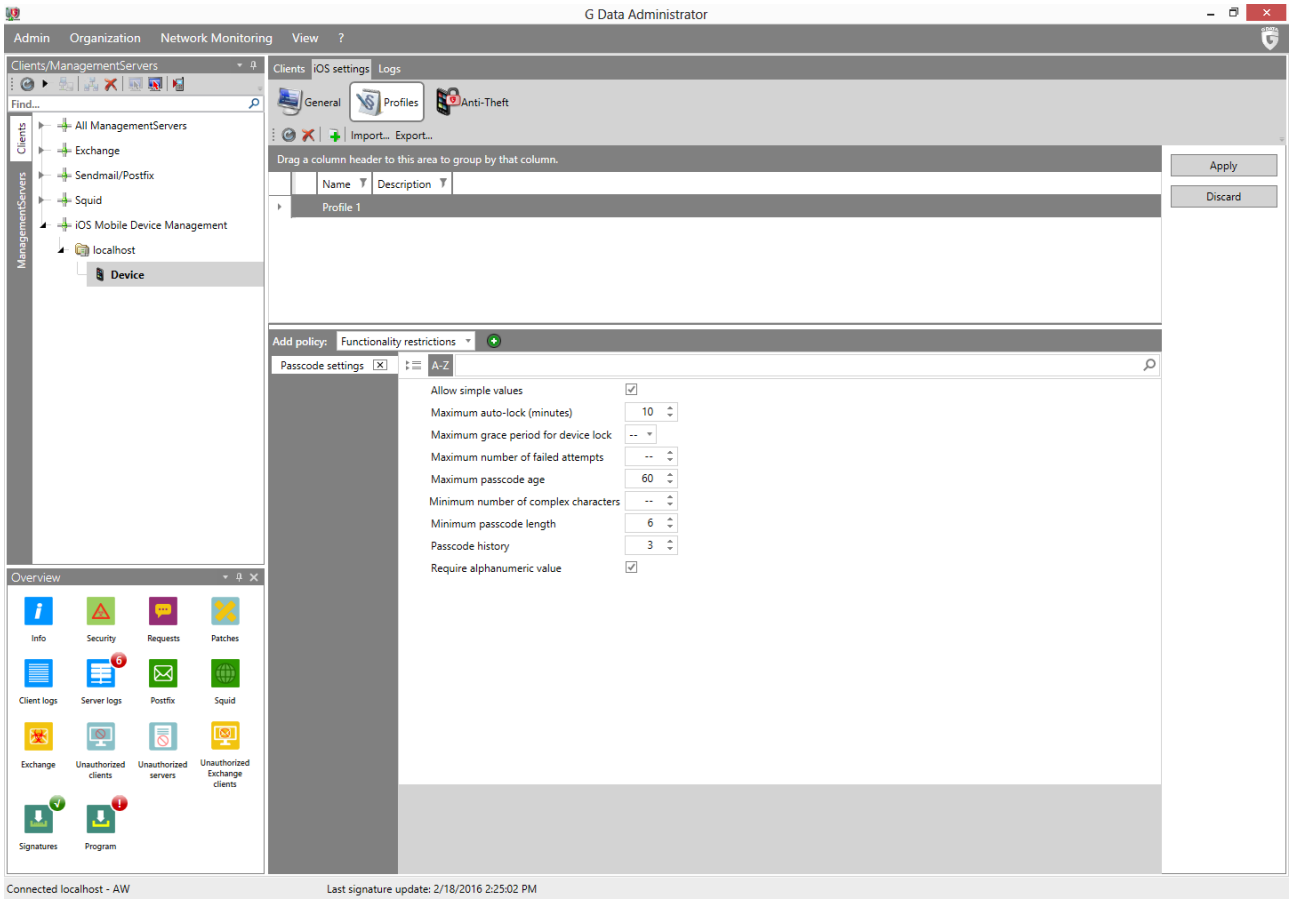


Image 7: G DATA Administrator, iOS settings, Profiles

Because Apple allows users to remove MDM profiles from their device at any time, administrators should make sure their security profiles contain a compelling reason not to do so. It is recommended to add the Wi-Fi policy to every profile. This allows the device to connect to the specified (protected) Wi-Fi network. When an end user tries to circumvent parts of the security policy by removing the MDM profile from an iOS device, Wi-Fi access is automatically removed, severely limiting the device's access to company resources. This makes sure that insecure devices do not have access to sensitive network shares or other confidential data.