



# avast! Mobile Security

## User Guide



## Contents

Welcome to avast! Mobile Security .....	4
System Requirements .....	5
How to install avast! Mobile Security .....	5
avast! Mobile Security Key Features .....	6
Virus Scanner .....	6
Privacy Advisor .....	7
Application Management.....	7
SMS and Call Filtering.....	7
Firewall - rooted phones only.....	8
avast! Mobile Security Settings.....	8
avast! Anti-Theft .....	9
Key Features of avast! Anti-Theft.....	9
Custom Name .....	10
Basic Settings.....	10
Advanced settings .....	11
Stealth mode .....	14
Remote Control .....	15
SIM card change notification .....	16
Call/SMS Forwarding.....	16
Retrieve Call Logs, Contacts, SMSes .....	17
Remote Siren.....	17
GPS Location Updates .....	17
Self-protection.....	18
Thorough wipe.....	18
Advanced Options .....	19
Uninstallation of avast! Anti-Theft .....	19
avast! Anti-Theft Commands .....	20
List of SMS Commands .....	21

## Welcome to avast! Mobile Security

avast! Mobile Security is a security solution specifically designed for Android devices. It consists of an Antivirus scanner to protect your smartphone from viruses and other malware, but also an Anti-Theft solution to help you recover your phone in the event that it is lost or stolen, and a number of other security enhancing features, such as the Privacy Advisor which allows you to see what personal data can be accessed by all your installed applications. You can also manage your applications and check what data they have access to, as well as filter calls and SMSes.

The antivirus scanner is based on a database of known virus signatures, which is regularly updated with the latest virus definitions to make sure you are protected from the very latest threats. On rooted phones, there is also the possibility to install a firewall, to restrict whether and how installed applications can access the internet.

The Anti-Theft feature allows you to control your phone remotely by sending simple SMS commands, for example to lock the phone or activate a siren. Alternatively, your phone can periodically and silently notify you of the phone's location, or forward details of both incoming and outgoing calls and text messages to another phone.

A key feature of Anti-Theft is that it works in stealth mode so that once activated, it is completely invisible to a potential thief and who would therefore be unaware of its activity. Furthermore, commands sent remotely, whether calls or SMS, will not be visible and will leave no trace on the stolen phone.

Even if the thief becomes aware of its presence, the Theft-Aware feature cannot be removed easily. And if the SIM card is changed, you will receive notification of the new number so that you will still be able to use the remote control commands.

The avast! Anti-Theft application is one of the best disguised anti-theft applications currently on the market!

## System Requirements

To run avast! Free Mobile Security your device must meet the following criteria.

### Operating Systems Supported

Android 2.1.x

Android 2.2.x

Android 2.3.x

### Minimum Hardware Requirements

Any phone capable of running a supported system

## How to install avast! Mobile Security

To install avast! Mobile Security, just download the installation file from the Android Market, then run the file to install avast! Mobile Security on your phone.

During the installation of avast! Mobile Security you will have the option to include the avast! Anti-Theft feature, or if it is not installed initially, there is the option within avast! Mobile Security to install it later when you select the Anti-Theft menu option. A simple installation wizard will guide you through the installation process.

You will also be asked to confirm if you wish to participate in the avast! Community. This is checked by default, but can be unchecked if you do not wish to participate. If you decide that you do wish to participate, certain security-related information will be forwarded to Avast Software, which may help to improve the protection provided to all users.

The same option can be found in the application Settings, so you can opt in or out at any time by checking or unchecking the box.

If your phone is rooted\*, you have the option to install Anti-Theft with root-privileges which will make it immune from a hard-reset.

You can then choose a custom name (or go back to obtain a random name suggestion) to disguise the installed application. This may be useful if your phone is stolen, as it will not be obvious to the thief that an anti-theft security application is installed.

Finally, press "Install". Before the installation proceeds, you will see a list of the data and services that Anti-Theft will have access to. If you wish to proceed, press "Install" again to complete the installation.

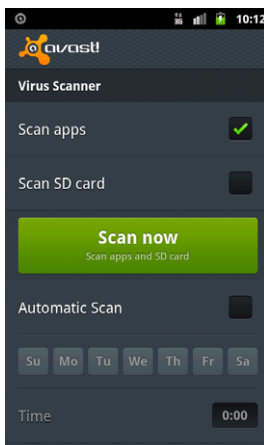
**Please note also that Android prevents uninstallation of device administrators. So if you are unable to uninstall Anti-Theft please double check that this setting is disabled in the Advanced Settings, then you should be able to uninstall as usual.**

\* **Rooted Phone:** An Android phone which has been switched (vendor enabled, hacked etc.) to a mode in which privilege control can be granted to an application. More information about how to root a phone can be found by carrying out a simple search on the Internet.

## avast! Mobile Security Key Features

avast! Mobile Security ensures your safety and privacy with a range of features to help ensure that personal data stored on your phone stays private and secure:

- Virus Scanner
- Privacy Advisor
- Application Management
- SMS and Call Filtering
- Firewall - rooted phones only
- Web Shield
- avast! Anti-Theft Integration



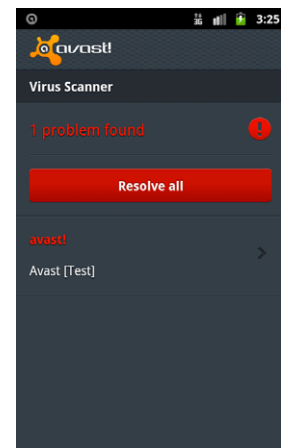
### **Virus Scanner**

avast! Mobile Security provides an “on-demand” virus scanner which is capable of scanning all installed applications and/or memory card content. There’s also an on-access scanner which automatically scans applications immediately after they are installed.

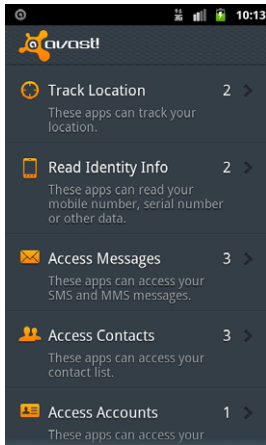
You can also schedule a scan to be run automatically once a day (on one or more days of the week) at a specified time. Note that in order to schedule a scan, at least one of “Scan apps” and “Scan SD card” must be selected. If anything suspicious is found, you will have the options to uninstall the application or delete the file.

If anything suspicious is detected, you will see a red button at the top of the screen informing you of a “problem”. Tap the red button to see what was detected.

You can then “Resolve all”, which will automatically delete or uninstall all files/applications detected as suspicious, or tap on an individual application or filename which will give you the option to either remove the file or application (e.g. “Uninstall”) or to send details to the avast virus lab in the case that it is a false alarm. This will enable us to update the virus database to prevent any recurrence of the false positive detection.



The virus definitions are updated automatically several times per day but it is also possible to update them manually if you want to be sure that you have the most up to date definitions at any given moment.



## Privacy Advisor

avast! Mobile Security also provides a scanner which checks the access rights and intents of installed applications. It will provide you with a list, showing the number of applications which can: Track your location, Read your Identity Information, Access your Messages, Access your Contacts, Access your Accounts, or Access Web Pages.

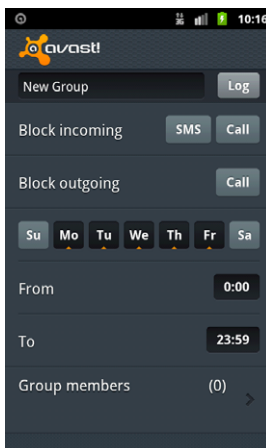
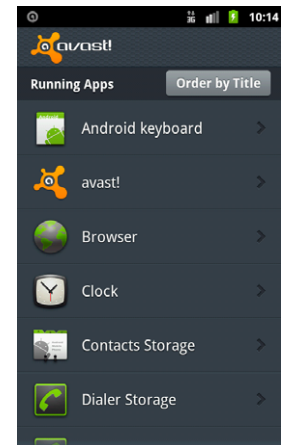
By selecting any one of these, you can then see a list of the specific applications. The Privacy Advisor thus identifies possible risks which might be caused by a specific combination of rights and intents granted to an application.

New applications are also checked during the installation to determine their access rights and you will then have the option whether or not to proceed.

## Application Management

Here you can see a list of all running applications. For each application, you can see its size (in MB), current CPU load, used memory, number of threads and services. To change the order in which the applications are listed, press "Order by Title" and select the new parameter by which you want them to be listed.

In "System Info" you can see how much space the application is using up. You can also kill the application by pressing "Force stop" or you can uninstall it completely. By scrolling down you can see what access rights the application has to all your other files, settings and personal data.



## SMS and Call Filtering

Within avast! Mobile Security, it is possible to block SMSes and/or calls from people in your contact list. The filtering is based on a set of rules (groups of contacts) which define when it is active: certain days of the week, a start time and an end time. The rule is active (selected contacts are filtered) on the selected days and within the specified time range.

You can block incoming Calls and/or SMSes and you can also block outgoing calls. Note however that numbers that contain less than 6 digits will not be blocked, to ensure continued access to emergency services. If an incoming call is blocked, the call is terminated and recorded in the SMS and Call Filter log.

Note that in order to block a particular number or group of numbers, it is necessary first to create a group and then add the required number or numbers by pressing "Add a New Group Member". Once a group has been created, you can then apply the required filter.

## Firewall - rooted phones only

With the avast! Mobile Security firewall, if your phone is rooted, it is possible to deny an installed application access to the Internet.

Access can be restricted depending on the type of connection: you can enable/disable access while on WiFi, 3G, or roaming mobile networks.



Select this icon to enable WiFi connections.



Select this icon to allow 3G connections,



and select this option to allow roaming for other mobile networks.

It is also possible to specify the permitted type of internet connection for groups of applications, grouped according to their access rights.

## avast! Mobile Security Settings

### Automatic updates

Here you can see the current installed version and if the box is checked, your phone will automatically download and install any available updates whenever it is connected to the internet.

### Connection type

This allows you to specify the type of internet connection that is required in order to obtain automatic updates.

### Check for updates now

By pressing this button, you can manually check for any updates if you want to be sure that you have the latest version of the program and virus definitions at a particular moment.

### Password protection

This enables you to set a password to protect your avast! applications

### Change avast! password

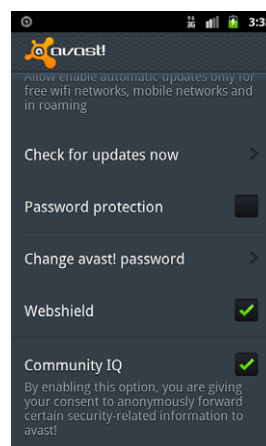
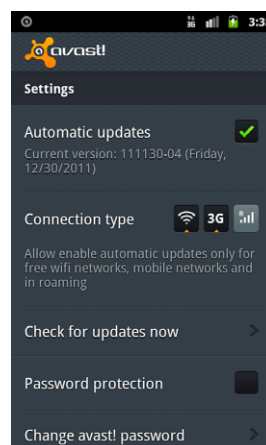
If your avast! applications are password-protected, the password can be changed here.

### Web Shield

The avast! Mobile Security Web Shield scans each URL which is navigated to from a web browser. If the URL is considered malicious, or if it is a known phishing site, a warning page is displayed. You can choose whether to continue to the URL or stay on the current page.

### Community IQ

Here you can change whether or not you wish to participate in the avast! Community.



## avast! Anti-Theft

avast! Anti-Theft can help you to recover your phone by controlling it remotely in the event that it gets lost or stolen. It is a separate but seamlessly integrated part of avast! Mobile Security and can be installed at the same time as the avast! Mobile Security product, or later as a separate installation. If it was not installed as part of the initial avast! Mobile Security installation, it can be installed later by choosing Anti-Theft in the main menu.

The stand-alone nature of the Anti-Theft component means it can operate in “stealth mode” so that it is completely invisible to a potential thief. Once the application is launched, it hides itself automatically, so that a potential thief is not even aware of its presence on your phone. This contrasts with other products on the market which are a visible part of the main product. This makes them almost redundant as any potential thief will dispose of a phone as soon he becomes aware of the Anti-Theft application, significantly reducing your chances of successfully recovering it.

### ***Key Features of avast! Anti-Theft***

- Custom Name – allows you to rename the application to disguise its real purpose
- Stealth Mode – automatically hides itself on your phone whenever it is activated so that a thief is not even aware of its presence
- Remote Control – you can control your phone remotely using specific SMS Commands in the event that it is lost or stolen
- SIM card change notification – notifies you automatically of the new number, if the SIM card is changed, so that you can still maintain contact with your phone
- Call/SMS forwarding – obtain details of calls made and received, copies of SMSes or get your phone to call you back so you can silently listen in.
- Retrieve call logs, SMSes – recover your personal data from your phone before wiping it
- Remote Siren – a siren can be activated remotely by SMS command
- Lock Screen Customization – you can specify the message to be displayed on screen when the phone is locked
- GPS Location updates – GPS can be automatically enabled so you can receive continuous GPS location updates
- Self Protection – difficult for a thief to modify or uninstall, can even survive a hard reset
- Thorough wipe – You can remotely wipe your phone clean, to protect your personal data.

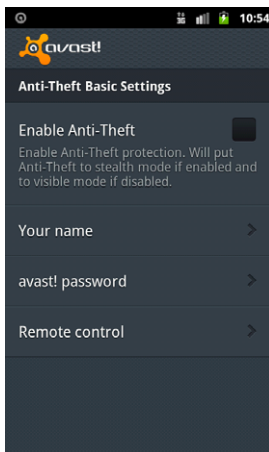
## **Custom Name**

The longer a thief is unaware that an anti-theft application is installed on your phone, the longer you will be able to keep control of it and the higher your chances of getting it back. Therefore, even before you download the avast! Anti-Theft application, you can choose a disguised name for it. The reason for this is to avoid drawing unwanted attention to it, or to avoid arousing suspicion that an anti-theft application is installed, for example, it could be renamed something like "Dodo Gadget".

The installation file is renamed with the custom name and the renamed application can then be installed. In future, whenever you search for your Anti-Theft installation, look for it by this disguised name.

## **Basic Settings**

Once installed, you will need to personalize your avast! Anti-Theft settings. You only need to specify a few basic settings; the advanced settings are already preconfigured but may be changed according to your preferences.

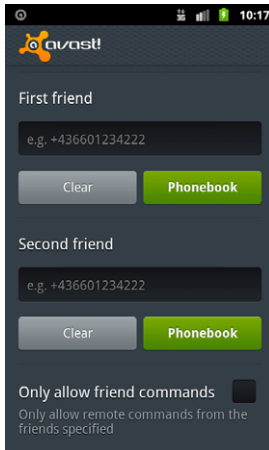


First of all, enter YOUR NAME to set up the owner of the device.

Secondly you will have to create your AVAST! PASSWORD which should be from 4 to 6 digits.

It is important to remember the password in order to continue to access Anti-Theft because once the Anti-Theft protection is enabled, as an additional protection measure, avast! Anti-Theft will hide itself from the app launcher and you will not be able to launch the program from there. Whenever you CALL this avast! password, in the same way as you would call a phone number, this call will be interrupted and Anti-Theft interface will be opened immediately.

Additionally the password is used to authorize SMS commands sent to your phone. Every SMS command begins with that password and ensures that the SMS will not be visible. If the password is wrong, the SMS command will be treated as a standard SMS and will be visible in your SMS inbox as normal.



Thirdly, in order to use the REMOTE CONTROL features of avast! Anti-Theft, you will need to specify one or two phone numbers of friends or family members who will receive the Anti-Theft notifications from your phone.

Check the box “only allow friend commands” to allow SMS commands only from the specified friend’s numbers, or, if left unchecked, SMS commands will be accepted from any number.

Now Anti-Theft is ready to go. Enable Anti-Theft by checking the option in the basic settings menu and Anti-Theft will be actively protecting your phone and can help you to recover it in the event of loss or theft.

## Advanced settings

In the advanced settings, you can further fine-tune how avast! Anti-Theft behaves:

### 1. Protection Behavior

***You can use these settings to specify the behavior of avast! Anti-Theft if the SIM card is replaced with a new, unknown SIM card, or if the phone is marked as “Lost” by sending a “LOST” SMS.***

#### **Lock phone**

If this option is enabled, the phone will be completely locked, making it impossible for a thief or other unauthorized user to access your phone or to uninstall avast! Anti-Theft using the application manager. This will increase battery usage, but also significantly increases your phone’s protection.

The phone can also be locked remotely by sending the “LOCK” SMS command.

#### **Sound siren**

If this option is enabled, a siren alarm will be sounded whenever the phone is locked, and will only stop when the phone is unlocked again. The siren can also be triggered by a remote SMS command.

#### **Deny program manager**

If this option is checked, it will not be possible to access the Program Manager. If the Lock phone option is enabled, access to the program manager will be automatically blocked.

#### **Deny phone setting access**

If this option is checked, access to all phone settings will be blocked, including the Program Manager. If the Lock phone option is enabled, this will automatically block access to everything, including your phone settings.

#### **Prevent USB access**

If this option is selected, USB debugging will be locked to prevent a thief or other unauthorized user from accessing the phone using special tools.

**Force data connection on**

By enabling this option, you can force the phone's data connection to remain open thus ensuring it remains reachable via the internet for as long as possible.

**Low battery notification**

If this setting is enabled, and the battery level is low, a notification SMS will be sent automatically to the numbers that you specified as friends in the basic settings. This gives you some advance warning before you lose contact with your phone.

**2. Lock Text, GPS, Wipe****Custom lock text**

Here you can also specify custom text to be displayed on the lock screen (e.g. offering a reward for finders) and you can change the text remotely using one of the remote control SMS commands.

**Automatically enable GPS**

If this option is selected, and GPS is not already activated on the phone, avast! Anti-Theft will attempt to activate GPS automatically whenever it needs to obtain GPS location data. This might be upon an unauthorized change of SIM card, or an SMS command requesting location data.

This is described in more detail on page 17.

**Thorough wipe**

If this option is selected, avast Anti-Theft will permanently and irreversibly delete the content of any SD card when wiping the phone.

This is described in more detail on page 18.

**Device admin**

This allows you to set avast! Anti-Theft as a Device Administrator, which will enable it to perform a full factory reset to permanently delete all your data.

**3. Siren sound**

The option "Select Sound File" allows you to select a sound file from your phone which will be played whenever the siren is activated. You may also be able to record a new sound using the option "Record Siren Sound", however this option is not supported on some devices. Use the option "Play Siren Sound" to listen to the currently selected sound or select "Reset to Default" to restore the original siren sound.

**4. Hard reset protection****Store settings**

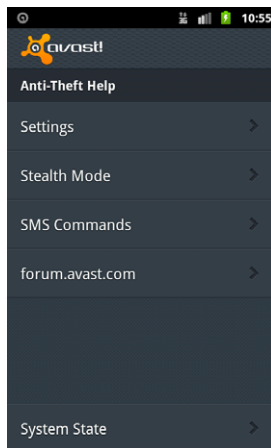
This setting applies only to rooted phones and enables the Anti-Theft settings to also be stored rooted so that they will even survive a hard reset.

**Check stored settings**

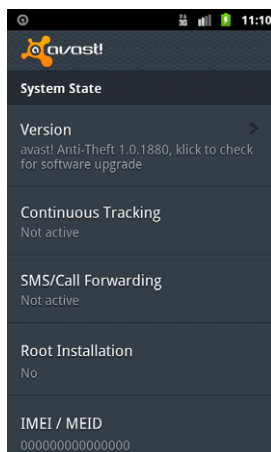
This enables you to check whether your settings were stored correctly.

## 5. Software updates

By selecting "Version", you can check whether you have the latest version of avast! Anti-Theft. Your phone can also carry out an automatic weekly check whether any updates are available, to ensure you always have the latest version. This will be done only if the SIM card is a trusted SIM card and the phone has not been marked as "Lost".



Pressing **Help, System State** at the bottom of the screen allows you to access the help files on your phone, including a list of all the available SMS commands...



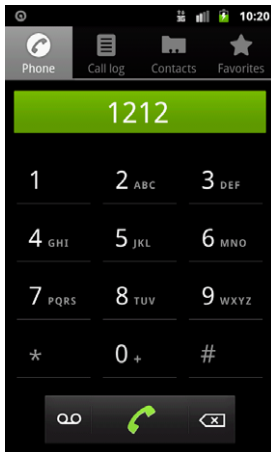
... and if you select System State you will see a list of the currently active system settings, such as Continuous GPS Tracking, SMS/Call Forwarding, whether GPS auto-enabling is set etc. These are all described in the following pages.

## Stealth mode

A very special feature of avast! Anti-Theft is the so-called stealth mode. Anti-Theft is the only solution in the marketplace that will automatically hide itself on the phone, in order to give you the best chances to catch the thief, or at least to get your device back.

Thieves usually check stolen phones for applications that could unveil their identity. They will look for application icons and will check the application manager. If the thief finds any trace of such an application, it is very likely that the phone will be turned off and will be subject to disposal. This usually results in the phone being lost forever.

Anti-Theft disguises itself first of all using a customized application name, but further hides itself by removing the Anti-Theft application launcher icon when the Anti-Theft protection is enabled so that it is completely invisible.

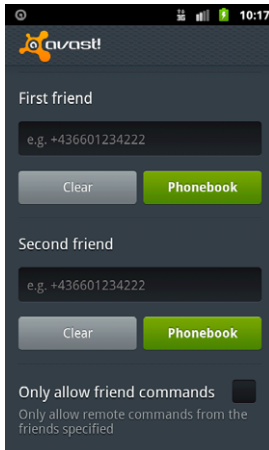


In stealth mode, because the application is hidden, you cannot launch the Anti-Theft interface in the usual way. Instead, you just need to **CALL the avast! password**, in the same way as you would call a regular phone number. For example, if your avast! password is set to 1212, just make a call to 1212. The call will be cancelled immediately without any cost to you and avast! Anti-Theft will start up within a few seconds.

To make Anti-Theft fully visible again, you just need to disable the Anti-Theft protection within the basic settings. This will restore the Anti-Theft application launcher icon instantly.

## Remote Control

To enable communication with your phone, you can register up to two notification numbers in avast! Anti-Theft e.g. your second phone plus the phone of a friend or family member.



In the event that your phone is lost or stolen, those phones will receive all messages sent by avast! Anti-Theft from your lost phone. You can also send various commands to your phone by SMS from any other phone with SMS capability, however, if you selected “Only allow friend commands” in the basic settings, SMS commands will be accepted only from those numbers. To remove that restriction, you should de-select the option.

Using the SMS commands, you can silently retrieve details of calls made and received, copies of incoming or outgoing SMS messages, you can remotely lock your phone, sound a siren or even remotely wipe your phone of all your personal data if you do not expect to recover it. You can also receive continuous GPS updates so that you can track your phone’s location. All of the available SMS commands are described later in this guide.

## SIM card change notification

Usually, some time after a phone is stolen, the thief may change the phone's SIM card. As you would normally not know the new phone number, you would then lose the ability to contact your phone and control it using the SMS commands. However, avast! Anti-Theft will recognize the SIM card change and will send the new phone number, plus the phone location data, to the friend or family member's phone number that you specified. The sender number of the SMS will be the phone number of the new SIM. Anti Theft will also try to locate the phone and add a map link to the notification SMS so that the recipient can see where the phone is located at that moment.

You can test if your notification numbers have been entered correctly by pressing the main menu button and selecting "Send test SMS". If everything is set up correctly a test SMS will be sent to the number or numbers that you specified.

There is also an option in the advanced settings to automatically lock the device (and optionally sound a siren) whenever a SIM card change is detected, however this would of cause alert the thief to the fact that an anti-theft application is installed. This can also be tested by selecting "Simulate lock" from the main menu.

You can set up avast! Anti-Theft so that it will trust more than one SIM card. The currently inserted SIM card will be added to a list of trusted SIM cards whenever you access the Anti-Theft interface. To accept another SIM card, just make sure the auto-lock feature in the advanced settings is turned off, then turn off the phone and change the SIM card as usual. After turning the phone back on, start up the Anti-Theft interface and the new SIM card will be automatically accepted.

You can clear the list of trusted SIM cards at any time by going to the main menu and selecting "Clear SIM list". This will leave the current SIM card as the only trusted one.

## Call/SMS Forwarding

Avast! Anti-Theft enables calls and/or SMSes to be forwarded or copied to another device by sending a simple SMS command.

*Calls:* whenever an incoming call arrives, SMS information about the incoming call will be sent to the remote control phone - calls will NOT be diverted!

*SMSes:* whenever an incoming SMS arrives, it can either be forwarded and deleted (will not arrive on the original phone) or if "CC" is set, the SMS will be forwarded and also delivered on the original phone.

You can also make a silent call to your phone using the CALL command which allows you to listen to what is going on at the other end of the line without the other person being aware.

## Retrieve Call Logs, Contacts, SMSes

By sending a simple SMS command, you can query the call log, the contacts and the SMSes saved on the phone. Each contact, SMS and call log entry will be forwarded as a separate SMS to the other phone. It is possible to filter the request for specific phone numbers, sent/received messages etc to limit the number of SMSes that will be sent. This ensures you will not lose all your personal data, even if you decide to wipe your phone.

## Remote Siren

Anti-Theft offers the option to remotely sound a loud siren on the device by sending a simple SMS command. As long as the phone is on, the siren sound will be played. If the volume of the external speaker is reduced, it will automatically be reset to maximum again after a very short time. The siren sound can also be customized by recording your own siren sound, or selecting a pre-recorded sound from a file.

## GPS Location Updates

As mentioned previously, Anti-Theft will recognize any SIM card change and will automatically send the new phone number to your friend's or family member's phone. If GPS is enabled, it will also include GPS location information. You can also use the "LOCATE" SMS command which will trigger the same positioning behavior. You can request the position just once, or you can specify the frequency for continuous updates.

In the advanced settings, you can select the option to "Automatically enable GPS" if GPS is not already enabled in the main phone settings.

Note however that while "on-demand" GPS updates will always work if Anti-Theft was installed rooted, there are some restrictions on non-rooted phones. On non-rooted phones the auto-enabling only works from Android 1.6 up to Android 2.2. For Android 2.3 and later, it is not possible to auto-enable GPS and therefore it is not possible to use the SMS Command to obtain GPS Updates.

It should also be noted that on non-rooted phones, the GPS auto-enabling can cause unwanted popups on the phone. This is the reason why on non-rooted phones you can choose if you want to use the GPS auto-enabling, or not.

To test whether popups occur, change the Anti-Theft settings so that GPS can be auto-enabled then make sure that GPS is disabled in the main system settings. To test if those popups occur, access the Anti-Theft main screen, press the menu key and select "Simulate Theft Event". If popups occur it is recommended to keep this setting disabled, otherwise you may draw attention to the fact that an anti-theft application is installed.

Note that keeping the auto GPS setting enabled will not consume power. This setting simply enables the GPS positioning to be activated, it does not actually activate it. Power from the battery will be used only while the GPS positioning is actually activated.

## Self-protection

Especially on rooted phones Anti Theft does everything to protect itself. As well as disguising and hiding itself, if Anti Theft is installed rooted, it cannot be uninstalled easily and even survives hard resets.

However, for this to work it is not enough just to install Anti-Theft in rooted mode because then, while the application itself would survive a factory reset, the application settings would be deleted.

The solution is to also store the Anti-Theft settings in rooted mode. So, once you are done with setting up Anti-Theft as you want it, as a last step you need to store the settings hard-reset-proof. To do this, you need to go to the Advanced Settings and from there select "Hard-reset protection" then "Store settings". There is a wizard to guide you through this so it should be quite straight forward. However, do not forget to do the hard-reset store every time you modify your Anti-Theft settings, otherwise any changes will be lost following a factory reset.

Within the advanced settings, there are additional Protection behavior settings to control how avast! Anti-Theft will behave in the event that the SIM card is replaced with a new unknown SIM card, or if the phone is marked as "Lost". For example, it can lock the phone, prevent access to the program manager and phone settings, prevent USB access, and even force the data connection to stay open.

From Android 2.2 on, it is also possible to set avast! Anti-Theft as a Device Administrator. As long as this setting is enabled in the advanced settings, the application can NOT BE UNINSTALLED.

## Thorough wipe

Wiping the phone can also be carried out by SMS command, if you do not expect to get your phone back and you do not want the thief to be able to access your personal data.

Up to Android 2.1, the wipe is somewhat restricted as a factory reset of the phone is not possible. However, Anti-Theft will try to delete as much as possible, for example contacts, call logs, SMS/MMS, browser history and SD card content, but not emails or apps.

From Android 2.2 onwards, a full factory reset is possible so you have full wipe capabilities. However please be aware that this will also delete avast! Anti-Theft, unless it was installed as a rooted application. To do a full wipe, Anti-Theft needs to be configured in the advanced settings as a device administrator, otherwise applications, emails etc will not be deleted.

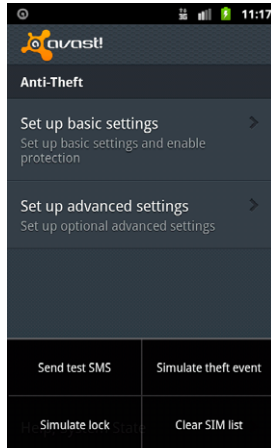
Whenever Anti-Theft wipes the phone, any SD cards will also be deleted. When doing a standard wipe, only the file directory would be deleted. This is the fastest way, but sophisticated thieves would be able to restore the deleted data using special tools.

The thorough wipe will take up to ten minutes, but will physically and irrecoverably delete the actual contents of your SD card. It is your choice whether to select the maximum level of security by using the thorough wipe option.

## Advanced Options

The Anti-Theft advanced options allow you to carry out various tests to verify that your phone has been set up correctly and will behave in the way expected.

To access the advance settings, just press the main menu button.



**Send test SMS** – This will send an invisible SMS to the friend numbers which you provided in the basic settings.

**Simulate lock** – this will simulate the LOCK SMS command and if successful, will lock the phone for 10 seconds.

**Simulate theft event** – this will carry out all the actions that should be performed if your phone SIM card is changed or if your phone is marked as "LOST". It will send an SMS to the provided friend numbers, however it may take some time as it will also try to obtain GPS location data.

The **Clear SIM list** button allows you to delete the list of trusted SIM cards, leaving only the current SIM card as the trusted one.

## Uninstallation of avast! Anti-Theft

Normally, avast! Anti-Theft can be uninstalled very easily through the Application Manager. Just select avast! Anti-Theft then press "System Info" then "Uninstall".

However, please note that Android devices do not allow device administrators to be uninstalled. So if you are unable to uninstall Anti-Theft please check the Advanced Settings and make sure that this setting is disabled, then you should be able to uninstall as usual.

## avast! Anti-Theft Commands

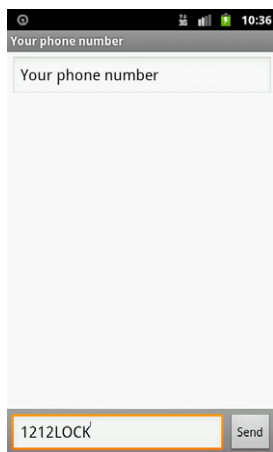
avast! Anti-Theft allows you to remotely control your phone using simple SMS commands. For this, the Anti-Theft protection needs to be enabled within the Anti-Theft basic settings.

Anti-Theft commands can be sent from another mobile phone with SMS capability.

If in the remote control settings, you specified certain friend's phones from which SMS commands can be sent, SMS commands will only be accepted if they are sent from a phone number that matches one of the friend's phone numbers that you specified. All SMS commands sent from other numbers will be ignored.

To see the full list of SMS commands on your phone, press Help and then choose "SMS Commands"

### SMS COMMANDS



All SMS commands must begin with your avast! password. For example, if your avast! password is set to 2222, a lock command should look like this: 2222 LOCK

If the option "Only allow friend commands" is selected, SMS commands will only be accepted if they are sent from one of the notification numbers provided. Any SMS commands sent from any other numbers will be ignored. If you want SMS commands to be accepted also from other numbers, this option should be de-selected.

If sent correctly, remote SMS commands will not cause any ring tone, signal, ambient light activation or any other indication of an incoming message on the target phone. Also, the SMS will not be visible in the SMS Inbox of the target phone and SMS replies sent back to you will also be sent silently and will not be stored in the Sent Messages outbox.

Note however that if the password is not correct, the command will be ignored and the SMS will be delivered to your phone's Inbox as a normal SMS and triggering the usual SMS arrival notification.

### List of SMS Commands

<p><i>LOST</i> Sample: 2222 LOST</p>	<p>Marks the phone as LOST. This command initiates the same actions as a SIM card change, depending on the protection behavior settings.</p>
<p><i>FOUND</i> Sample: 2222 FOUND</p>	<p>Marks the phone as FOUND. This command disables the phone lock as well as the siren alarm.</p>
<p><i>LOCK</i> Sample: 2222 LOCK</p>	<p>Locks the mobile phone</p>
<p><i>UNLOCK</i> Sample: 2222 UNLOCK</p>	<p>Unlocks the mobile phone</p>
<p><i>MESSAGE</i> &lt;message text&gt; Sample: 2222 MESSAGE Give back my phone!</p>	<p>Will display a message on the phone. However, such a message can simply be dismissed. Or use SET LOCKTEXT to create a "sticky" message that will be displayed when the phone is locked, then use "LOCK" to lock the phone and trigger the message</p>
<p><i>SIREN ON</i> Sample: 2222 SIREN ON</p>	<p>Turns the siren on</p>
<p><i>SIREN OFF</i> Sample: 2222 SIREN OFF</p>	<p>Turns the siren off</p>
<p><i>LOCATE</i> Sample: 2222 LOCATE</p>	<p>Requests new location data</p>
<p><i>LOCATE</i> &lt;interval duration in minutes&gt; Sample: 2222 LOCATE 5</p>	<p>Requests location data every 5 minutes</p>
<p><i>LOCATE STOP</i> Sample: 2222 LOCATE STOP</p>	<p>Stops continuous location updates</p>
<p><i>CALL</i> [phone number] Sample: 2222 CALL Sample: 2222 CALL +43660333555</p>	<p>If no phone number is given this command causes the phone to call you back. If you give the phone number the phone will call the given number</p>
<p><i>FORWARD SMS</i> [phone number] Sample: 2222 FORWARD SMS Sample: 2222 FORWARD SMS +43660333555</p>	<p>If no phone number is given, incoming SMS will silently be forwarded to the phone that sent the command and deleted (will not be delivered) on the original target phone. If a phone number is given, incoming SMS will be forwarded to the given phone number. This command overrides all previously issued SMS-forwarding-settings. The forwarding can be cancelled by issuing the <i>FORWARD SMS STOP</i> command or you will have the option to cancel the instruction whenever you launch the avast! Anti-Theft interface.</p>
<p><i>CC SMS</i> [phone number] Sample: 2222 CC SMS Sample: 2222 CC SMS +43660333555</p>	<p>Same as FORWARD SMS, but will not delete the SMS after forwarding which means that the forwarded SMS will still be delivered to the target phone (CC means carbon copy). This command overrides all previously issued SMS-forwarding-settings.</p> <p>The forwarding can be cancelled by issuing the <i>CC SMS STOP</i> command or you will have the option to cancel the instruction whenever you launch the avast! Anti-Theft interface.</p>

<p><i>CC CALLS [phone number]</i>  Sample: 2222 CC CALLS  Sample: 2222 CC CALLS  +43660222333</p>	<p>By issuing this command you can request SMS notifications about incoming calls. The notifications will be sent to the phone that issued the command if no other phone number is given. This command overrides all previously issued call-forwarding-settings.</p> <p><i>calls cannot be forwarded as this works differently in networks around the world. Also it is not possible to reliably hide the call forwarding settings.</i></p> <p>The notifications can be cancelled by issuing the <i>CC CALLS STOP</i> command or you will have the option to cancel them whenever you launch the avast! Anti-Theft interface.</p>
<p><i>CC ALL [phone number]</i>  Sample: 2222 CC ALL  Sample: 2222 CC ALL  +43660222333</p>	<p>Combines the CC SMS and the CC CALLS command. This command overrides all previously issued SMS- and call-forwarding- settings.</p> <p>The forwarding can be cancelled by issuing the <i>CC ALL STOP</i> command or you will have the option to cancel the instruction whenever you launch the avast! Anti-Theft interface.</p>
<p><i>WIPE</i>  Sample: 2222 WIPE</p>	<p>Wipes all data from the phone</p>
<p><i>GET &lt;query limit&gt; SMS</i>  Sample: 2222 GET 10 SMS</p>	<p>Gets the last 10 SMS messages</p>
<p><i>GET &lt;query limit&gt; INBOX SMS</i>  Sample: 2222 GET 10 INBOX SMS</p>	<p>Gets the last 10 received SMS messages</p>
<p><i>GET &lt;query limit&gt; SENT SMS</i>  Sample: 2222 GET 10 SENT SMS</p>	<p>Gets the last 10 sent SMS messages</p>
<p><i>GET &lt;query limit&gt; SMS FOR &lt;phone number&gt;</i>  Sample: 2222 GET 10 SMS FOR  +43660333555</p>	<p>Gets the last 10 SMS messages matching the phone number given</p>
<p><i>GET CONTACTS</i>  Sample: 2222 GET CONTACTS</p>	<p>Gets the contacts from the address book</p>
<p><i>GET LOG &lt;query limit&gt;</i>  Sample: 2222 GET LOG 10</p>	<p>Gets the call and SMS log</p>
<p><i>LAUNCH</i>  Sample: 2222 LAUNCH</p>	<p>Launches the avast! Anti-Theft user interface</p>
<p><i>CLOSE</i>  Sample: 2222 CLOSE</p>	<p>Closes the avast! Anti-Theft user interface</p>
<p><i>REBOOT</i>  <i>(only for rooted devices)</i>  Sample: 2222 REBOOT</p>	<p>Reboots the device</p>
<p><i>SET OWNER &lt;name of owner&gt;</i>  Sample: 2222 SET OWNER  Charles Chaplin</p>	<p>Will change the device owner name</p>

<i>SET PASSWORD</i> <access code> Sample: 2222 SET PASSWORD 3333	Will change the avast! password. You will need to provide a password of 4-6 digits
<i>SET FRIEND 1</i> <phone number> Sample: 2222 SET FRIEND 1 +43660122220192	Will change the phone number of the first friend. Provide a valid mobile phone number
<i>SET FRIEND 2</i> <phone number> Sample: 2222 SET FRIEND 2 +43660122220192	Will change the phone number of the second friend. Provide a valid mobile phone number
<i>SET ONLYFRIENDS</i> <friends mode> Sample: 2222 SET ONLYFRIENDS 1	Will change the SMS command authorization mode (0 = allow all numbers, 1 = allow only friend commands)
<i>SET LOCKMODE</i> <lock mode> Sample: 2222 SET LOCKMODE 1	Will change the phone lock protection behavior (0 = do not lock, 1 = auto lock)
<i>SET SIRENMODE</i> <siren mode> Sample: 2222 SET SIRENMODE 1	Will change the siren protection behavior (0 = no siren on lock, 1 = siren on lock)
<i>SET APPLOCKMODE</i> <app lock mode> Sample: 2222 SET APPLOCKMODE 1	Will change the program manager or phone setting protection behavior (0 = no setting active, 1 = deny program manager, 2 = deny phone settings)
<i>SET USBLOCKMODE</i> <USB lock mode> (only for rooted devices) Sample: 2222 SET USBLOCKMODE 1	Will change the USB protection behavior (0 = do not lock USB access, 1 = lock USB access)
<i>SET FORCEDATAMODE</i> <force data mode> (only for rooted devices) Sample: 2222 SET FORCEDATAMODE 1	Will change the force data connection protection behavior (0 = do not force data connection, 1 = force data connection)
<i>SET BATTERYSMSMODE</i> <battery mode> Sample: 2222 SET BATTERYSMSMODE 1	Will change the low battery notification protection behavior (0 = do not notify on low battery, 1 = notify on low battery)
<i>SET LOCKTEXT</i> <lock text> Sample: 2222 SET LOCKTEXT Please call me back at +4313283483	Will change the custom lock text
<i>SET AUTOGPS</i> <gps mode> Sample: 2222 SET AUTOGPS 1	Will enable or disable automatic enablement of GPS (0 = turn off, 1 = turn on)
<i>SET WIPEMODE</i> <wipe mode> Sample: 2222 SET WIPEMODE 1	Will enable or disable thorough wipe (0 = turn off, 1 = turn on)
<i>SET PROTECTION</i> <protection mode> Sample: 2222 SET PROTECTION 1	Will enable or disable Anti-Theft protection (0 = turn off, 1 = turn on) <b>Caution: By using this command you will completely disable the avast! Anti-Theft system thus rendering the Anti-Theft protection useless.</b>

**Thank you for choosing avast!**

