Mobile Security for Android 2.2–3.2 devices

1 Swisscom Mobile Security™ for Android 2.2–3.2 devices

This guide covers mobile devices (smartphones, tablets) that use the Android operating system (version 2.2 to 3.2). You can find out which mobile devices with this operating system have been tested with Swisscom Mobile Security at www.swisscom.com/f-secure.

2 Installing Mobile Security

2.1 Android devices with preinstalled Mobile Security software

If you buy your mobile device from Swisscom, the Swisscom Mobile Security software is partly preinstalled on it. In most cases the preinstalled software can be found in the *Applications (Apps) menu*. You can thus activate Mobile Security directly by selecting the padlock icon labelled Mobile Security. Please note that, depending on the type of mobile device, the name may appear in abbreviated form. When you open Mobile Security for the first time, you must activate it (see section 3) in order for your mobile device to be protected. The product does not protect your device until you activate it. You can choose to try out the software free of charge for a 30-day trial period before taking out a subscription with Swisscom.

2.2 Android devices with preinstalled Swisscom Security Launcher

If you have bought your mobile device from Swisscom, you may find the padlock icon with the title Swisscom Security Launcher (or a corresponding abbreviation) in your Applications (Apps) menu. This icon opens a dedicated download program (launcher) for the Swisscom Mobile Security software.
Please note that your mobile device will download about 2 MB of data when installing the software. It is therefore advisable to have a Swisscom subscription with a data option and ensure that you have access to the Swisscom network or a private WLAN while downloading. *Important:* First of all, make sure that you have set your mobile device to install programs from *unknown sources*. This is done in the *Settings* → *Applications* menu and can be turned off again after you have installed Mobile Security.
The Swisscom Security Launcher will lead you to this setting if you have not yet set your device to install programs from unknown sources. As soon as you have finished installing the software, you need to activate Mobile Security (see section 3). The software will not protect your mobile device until you have activated it. You can choose to try out the software free of charge for a 30-day trial period before taking out a subscription with Swisscom.

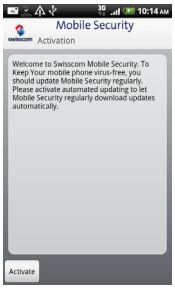
2.3 Android devices with no preinstalled Mobile Security or Swisscom Security Launcher

If you have bought a mobile device with no preinstalled Swisscom Mobile Security software or Swisscom Security Launcher, you can still install Swisscom Mobile Security. Your device does not have either of these apps if there is no Swisscom padlock icon in your mobile device's Applications (Apps) menu.
Important: First of all, make sure that you have set your mobile device to install programs from *unknown sources*. This is done in the *Settings* → *Applications* menu and can be turned off again after you have installed Mobile Security.
Open your Internet browser and type http://mobile.f-secure.com/swisscom into the address bar. You can start the download from the Web page that appears. Choose the Mobile Security download for Android 2.2–3.2. You will find the fully downloaded software in notifications on your mobile device. Activate the downloaded Mobile Security download software and follow the on-screen installation instructions to activate it.

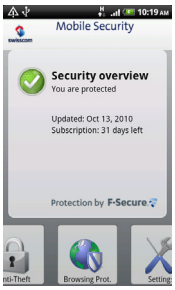
swisscom

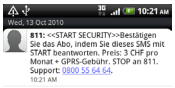
3 Activating/deactivating Mobile Security

3.1 Activating Mobile Security



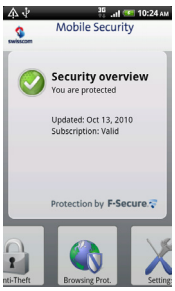
Activating the free trial of Mobile Security:
The first time you open Mobile Security, you can choose a 30-day free trial. The trial begins as soon as you activate Mobile Security for the first time.
Tap the Mobile Security icon, then *Activate*, and follow the on-screen activation instructions. When you activate the software, it needs to be updated from an update server. Use the *Swisscom Services* connection on the Swisscom mobile network to download the updates. The activation wizard then asks you to set up Mobile Security and scan your mobile for viruses. However, you can do this at any time.
If you have successfully activated Mobile Security, the remaining trial time is shown in the Mobile Security overview window. Mobile Security has the same functions as the paid subscription version for the duration of the trial. You can order a paid subscription directly from Swisscom at any point during the trial. Mobile Security will give you reminders seven and three days before the free trial runs out. To ensure that your mobile device remains optimally protected, we recommend taking out a subscription with Swisscom in good time.





Ordering a paid Mobile Security subscription (recommended option):

1. Open the *Mobile Security* application from your main or Programs menu. Mobile Security displays an overview showing how many days there are until your free trial runs out.
2. Select *Subscription*. You can see when your trial runs out and how much a Swisscom Mobile Security subscription costs per month.
3. Then tap the first button, *Continuous Subscription*, to order a subscription, which will be conveniently added to your own monthly Swisscom bill.
4. Mobile Security automatically texts *START SECURITY* (free of charge) to *811*, and you are then informed that you will receive confirmation of your order. You can see that your order has been accepted in the Mobile Security overview.
5. Now go to the *Messages* application, where you see your incoming text messages. There is a text message in your *Inbox* folder from *811* containing the words *START SECURITY* and explaining how to confirm your order. You are also informed once again how much the Mobile Security subscription will cost per month.
6. *Important*: Reply to this text message by texting *START* to the same number *(811)*. Your order is not completed until you send this reply.
7. You will then receive another text message from *811* in your *Inbox* folder containing confirmation of your order, the cost of the service and an explanation of how to cancel your Mobile Security subscription.
8. The Mobile Security overview page now shows your subscription.



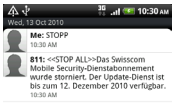
Alternative way to activate the paid Mobile Security subscription:
You can also order a Mobile Security subscription without starting the free trial by texting *START* to *811* from your text messaging application.
You will then receive a reply from 811 informing you that your order for a Mobile Security subscription has been accepted.

3.2 Deactivating Mobile Security (cancelling)

Cancelling the subscription by selecting Unsubscribe in Mobile Security *(recommended option):*

If you no longer want to use Mobile Security, select *Subscription* in your Mobile Security program.

1. Select *Continuous Subscription*.
2. Tap the *Unsubscribe* button. You can now see details of your Mobile Security subscription.
3. If you want to cancel your subscription with Swisscom, tap *Cancel*.
4. In the background, Mobile Security will text *STOP SECURITY* (free of charge) to *811* and tell you that the cancellation request has been sent and will be confirmed by text message.
5. A text message from 811 will now appear in your Inbox folder confirming the cancellation and informing you how long your Mobile Security subscription will remain valid.
6. The Mobile Security overview page now shows when your subscription will run out.



Alternative way to cancel your subscription by text message:

You can also cancel your subscription with Swisscom by texting any of the following to *811* from your text messaging application:

> STOP, STOPP
> STOP ALL, STOPP ALL
> STOP SECURITY

You will receive a text message from 811 informing you that your Mobile Security subscription has been cancelled and indicating how long the Mobile Security update service will remain available.

NB: texting STOP ALL also deletes your Mobile Security subscriptions for any guest devices (see section 3.4.2)

3.3 Details of your Swisscom Mobile Security subscription

You can receive details of your Mobile Security subscription at any time via text message by texting the following keywords to *811*:

> *HELP or INDEX*: You will receive a text message containing details of the service and the cost of your subscription.
> *INFO*: You will receive a text message containing the contact details for Swisscom and F-Secure support.
> *VIEW*: You will receive a text message indicating whether or not your Mobile Security subscription is still active.

3.4. Subscribing to and cancelling Mobile Security for a guest device

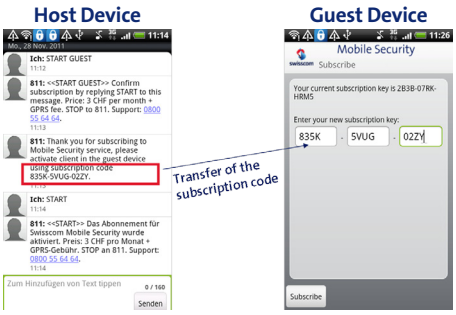
3.4.1 Subscribing to Mobile Security for a guest device (with or without SIM card)

With Mobile Security version 7.5 or later, you can also use this application on a mobile device

1. which is permanently operated without a SIM card, or
2. which is not permanently operated with a Swisscom SIM card, or
3. which is operated with a SIM card for another mobile network, or
4. whose monthly Mobile Security subscription fees you would like to pay.

You will find your Swisscom Mobile Security version number in the main menu under *About*. If you have an older version than 7.5, you can download the latest version *by* selecting Update in the main menu.

If your free 30-day trial has expired, you will be asked to subscribe to Mobile Security. Normally, you subscribe to the service by sending a text message to 811, as described in section 3.1, in order to add the service to your own Swisscom subscription. However, if you wish to operate a mobile device with Mobile Security in any of the four situations described above, you can register your mobile device as a guest device. To do this, you just need a mobile device (host device) with a Swisscom subscription, to which the cost of Mobile Security for your device will be assigned. This payment method is particularly convenient if you want to use a *tablet* exclusively on your home WLAN, without a SIM card, and still want to be protected from the dangers of the Internet.



1. From the mobile device (host device, see left-hand picture) to which the cost is to be assigned, text *START GUEST* (free of charge) to *811*.
2. Your host device will then receive an initial text message from *811*, asking you to send another text message to *811*. A second text message from *811* will then immediately arrive with a 12-digit *subscription code*.
3. You must then confirm the subscription again by texting *START* to *811* from the host device.
4. Your host device will then receive another text message from *811*, informing you that the subscription has been activated on the guest device.
5. Select *Subscription* on your mobile device (guest device). Then choose the second payment method, *Use subscription key*. In the following field (see right-hand picture), you can then enter the 12-digit subscription code that was sent to your host device. NB: Your host device can be assigned the cost of several guest devices.

3.4.2 Deactivating (cancelling) Mobile Security for a guest device

If the cost of your Mobile Security subscription has been assigned to another mobile device (host device), the service must also be cancelled on the host device concerned.

1. To do this, text *STOP GUEST <guest subscription code>* free of charge to *811* from the (host) mobile device to which the cost has been assigned.
2. The host device will then receive a text message from *811*, confirming the cancellation for the guest device. NB: Texting *STOP GUEST* without a subscription code will be treated as an invalid command.

3.4.3 Mobile Security details on a guest mobile device

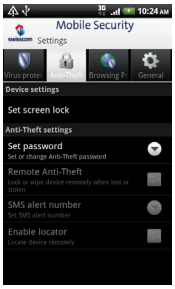
You can receive details of your Mobile Security subscription for a guest device at any time via text message by texting the following keywords to *811* from the host device. The relevant information will be texted to your host device.

- *HELP GUEST or INDEX GUEST:* the host device will receive a text message containing details of the service and the cost of the subscription for a guest device.
- *INFO GUEST:* the host device will receive a text message containing the contact details for Swisscom and F-Secure support.
- *VIEW GUEST:* the host device will receive a text message indicating whether or not the Mobile Security subscription for a guest device is still active.
  NB: if the host device has been assigned the cost for more than one guest device, the subscription code must be entered after the keywords in order to clearly identify the mobile device concerned, e.g. *VIEW GUEST <guest subscription code>*.
  NB: if you send this text message to 811 from the guest device, it will not work. The Mobile Security administrator does not recognise the guest device from its mobile telephone number, but only via the host device.

4 Mobile Security features

4.1 Anti-Theft

Anti-Theft protects your data against loss or theft so that it cannot be misused. It also allows you to locate your mobile device if it is equipped with a GPS receiver. You need a second trusted mobile device to control the Anti-Theft functions on your mobile device.
If you use a mobile device that does not allow text messaging, you cannot use Anti-Theft.



Locking your device:
Anti-Theft can automatically lock your device if the SIM card is changed. It can only be unlocked using your security code.

Setting up the locking function:
1. Select *Settings* in the main Mobile Security menu.
2. Select *Anti-Theft* in the Settings menu.
3. Select *Set Security Code*. The security code must be at least four characters long. Keep it safe.

Using remote Anti-Theft functions:
If your mobile device is lost or stolen, Anti-Theft allows you to text your security code to it from a second trusted mobile device so that you can locate it, lock it or wipe your data from it.

How to set up remote locking:
1. Open *Settings* from the main menu and press the selection key.
2. Select *Anti-Theft* in the Settings menu.
3. Follow these instructions if you want to be able to lock your device remotely:
   a. Select *Set Security Code* (at least four characters, see picture).
   b. Activate *Remote Anti-Theft*, which enables you to lock your mobile device remotely or wipe your data from it remotely. The locked device can only be unlocked using the security code.
   c. Under *Trusted number*, enter a trusted mobile device number from which you can send a text message. You need this mobile device number to lock your own device or wipe your data from it.
   d. Select *Enable locator* to ensure that your own device can be located from another device (i.e. the other device can receive your mobile's GPS coordinates).

How to lock and wipe your mobile remotely:
Send the following text messages from the trusted device to your mobile device number:
› To lock your mobile device: #LOCK#<security code> (e.g. #LOCK#abcd1234)
› To wipe your mobile device: #WIPE#<security code> (e.g. #WIPE#abcd1234)
Since memory cards can easily be removed, store your confidential data in your mobile's onboard memory. Anti-Theft will then allow you to lock or wipe the data.
Anti-Theft does not store any location data. Only the text message sent to the trusted device contains details of your mobile's location.

How to locate your lost or stolen mobile device from the trusted device:
› To find out where your mobile device is, text the following to your mobile device from the trusted device: #LOCATE#<security code> (e.g. #LOCATE#abcd1234)
› The trusted device will now receive a text message from your mobile device containing a link to Google Maps. If you are unable to view your mobile's location on the trusted mobile device, you can still see your mobile device's most recent GPS coordinates in the text message.

How to send your mobile device's location to friends and family:
› Select *Anti-Theft* from the main menu.
› Now select *Location sharing*.
› Your mobile device will now take the GPS coordinates from its GPS receiver and create a text message containing a link to its location on Google Maps.
› Enter the desired number in the text message's address line and select *Send*.
› The person who receives the text message can now use the link it contains to view your location or see the GPS coordinates directly in the message.

4.2 Scanning for viruses

As soon as you have activated Mobile Security for the first time, scan your mobile device to make sure that it is free from viruses and other harmful programs. You should always run a scan when the application prompts you to do so.
Swisscom Mobile Security runs in the background and scans your files automatically.

1. A message is displayed whenever a harmful program is found during the real-time scan. Tap *Yes* to view the infected file(s) or *No* to close the message.
2. The *Infected files* view lists the infected files found on your mobile device and shows the status of each file (quarantined or released).

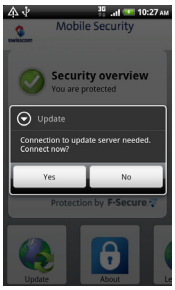
Follow these instructions to view further details of an infected file:

1. Scroll to the infected file and press the selection key.
2. Select *View*.
3. The infection details view shows the path and name of the infected file as well as the name of the harmful program that has infected it.

Process infected files as follows:

1. Scroll to the infected file you want to process in the *Infected files* view.
2. Press the selection key.
3. Select one of the following actions:
   - *Delete* – deletes the infected file. This is the recommended option. The file is completely removed from your device.
   - *Quarantine* – places the infected file under quarantine if it is not already under quarantine. A quarantined file is blocked and cannot harm your device as long as Mobile Security is activated.
   - *Release* – releases a quarantined file. The file is no longer blocked after you release it. You can access it, but you do so at your own risk.

4.3 Automatic updates



Swisscom Mobile Security includes an automatic update service that regularly updates its virus definition database. Only an up-to-date virus definition database can ensure that your device is protected against the latest viruses and other harmful programs. Automatic updates take effect once you have activated the software. The application needs an active Internet connection to download the updates. If an Internet connection is available, Mobile Security checks when the virus definition database was last updated and downloads new updates as appropriate. Please note that this involves data transfer, so you should only use this feature if you are on a network where the data transfer costs are included in your subscription or if you are connected to a private WLAN.

4.4 Manual updates

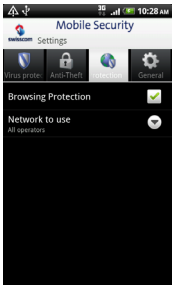
You can also carry out updates manually.

1. Select *Update* from Mobile Security's main menu.
2. When asked if you want to connect to the update server, answer *Yes*.
3. Choose the Internet access point for the connection to the update server. Please note that this involves data transfer, so you should only use this feature if you are on a network where the data transfer costs are included in your subscription. The application downloads the updated virus definition database and starts using it immediately.
4. Once the update has ended, tap *Yes* when prompted to scan your mobile for viruses. If a new version of Mobile Security is available, a message appears prompting you to download it. The application restarts automatically once the new version has been downloaded.

4.5 Using the Internet securely with Browsing Protection

Mobile Security also automatically installs a second Internet browser on your mobile device. It appears in the Apps menu as a symbol labelled *Browsing Prot*. Use this browser whenever you want to surf the Internet.
Browsing Protection allows you to see which websites are secure and avoid accidentally visiting harmful ones. As soon as you call a website up, the browser automatically checks how secure it is. If the website has been identified as suspicious or dangerous (phishing websites or those infected with harmful programs), Mobile Security blocks access to it. A website's security rating is based on information from several sources, including malware analysts and F-Secure partners.

You can also open Browsing Protection from Mobile Security. Select *Browsing Prot.* from the main menu and then *Safe browser. Important:* Browsing Protection is only active when you use this browser to surf the Internet. If you choose a different browser, you are not protected while you surf.
If you have activated Parental Control for your child, the mobile device will always use Browser Protection, even if your child tries to use a different browser.

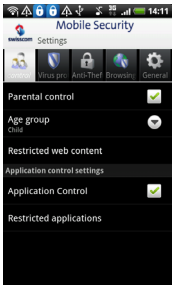


Changing Browsing Protection settings:
Select when Browsing Protection is to be used. This depends on the network you are using. Follow these instructions to change the settings:

1. Tap the *Settings* button in Mobile Security's main view and select *Browsing Prot.*
2. To activate Browsing Protection, change the *Browsing Prot.* setting to *On.* Mobile Security will now run in the background while you surf the Internet.
3. Select when Browsing Protection is to be used:
   - > *All operators* – the software checks the security of the websites you visit, regardless of the network you are using (see picture).
   - > *My operator only* – the software only checks the security of the websites you visit when you are using your own operator's network.

The software applies the new settings immediately. Mobile Security may prompt you to use the browser installed by the manufacturer as the default browser. To ensure that you can surf as securely as possible, you should change to the default browser recommended by Mobile Security.
You can check your device's Browsing Protection status at any time by tapping the *Browsing Prot.* button in Mobile Security's main menu.

4.6 Parental Control

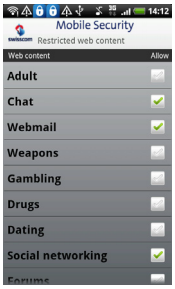


If you have version 7.5 or later, Swisscom Mobile Security includes parental controls which you can switch on if needed for your children or teenagers. You can find out which version of Swisscom Mobile Security you have by selecting *Learn more* in the main menu. If you have an older version than 7.5, you can download the latest version by selecting *Update* in the main menu.

Parental Control enables you to restrict the selection of websites available to your child. In the default setting, i.e. after Swisscom Mobile Security is activated, Parental Control is switched off.
You can find Parental Control in the Swiss Mobile Security main menu under *Settings* → *Parental Control* or in the main menu under *Parental Control* → *Settings* (see picture).

In the Parental Control menu, you can generally switch Parental Control on or off by checking or unchecking the box (first menu item). If you leave Parental Control switched off, you can continue to use the different Internet browsers that are installed on your child's mobile device. However, we recommend that your child always uses Browser Protection in order to remain protected from the dangers of websites infected with harmful programs and fraudulent (phishing) websites.

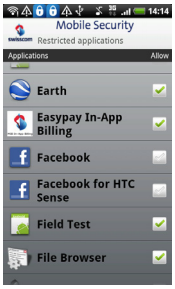
If you switch on Parental Control, regardless of the protection level, your child will only be able to use Browser Protection. If your child tries to use a different browser, Browser Protection will be opened automatically. This ensures that your child is not only protected from harmful software on infected sites, but also that he/she can only access websites in a category that you have allowed. In order to make any changes to these settings, you will be asked to type in a *Security Code* which only you (and not your child) should know. If you did not create this code when you switched on Swisscom Mobile Security for the first time, you can do so now.



Parental Control for teenagers:
Activate *Parental Control* and select *Teen* from the *Age group* menu. Under *Restricted web content* (third menu item), you will find the pre-set list of enabled and blocked website categories for teenagers. You can change the category list to suit your teenager by checking or unchecking the corresponding boxes in the *Allow* column (see picture).

Parental Control for children (see picture):
Activate *Parental Control* and select *Child* from the *Age group* menu. Under *Restricted web content*, you will find the pre-set list of enabled and blocked website categories for children. You can change the category list to suit your child by checking or unchecking the corresponding boxes in the *Allow* column.

Parental Control for adults:
You can select this option as an adult from the *Age group* menu either to temporarily remove Parental Control for your child or to give your teenager an adult category profile set by you. However, you can also select this age group in order to stop you or your teenager using a browser other than Browser Protection, which protects you from websites with harmful software.
What else do you need to know? If you have switched on Parental Control on your child's mobile device, regardless of the protection level, your child cannot use any other browser except Browser Protection. You or your child will also be asked to enter the Parental Control *security code* for certain applications or administrative tasks. The security code is required in order to prevent your child from bypassing the Parental Control security settings or trying, for example, to stop, deactivate or uninstall Swisscom Mobile Security. The security code is the same one that you use for the Anti-Theft facility.



Application Control
Mobile Security Parental Control also includes Application Control, which you can use to prevent your child from using particular applications (apps). Under *Restricted applications*, Parental Control searches for all installed apps and shows them initially as enabled. You can now block individual apps by unchecking the boxes under *Allow* (see picture). Note that you will need to enter the security code to make such changes. This is to prevent your child from reversing all the changes later on. The apps you have blocked are not uninstalled, but remain in the App Menu of your child's smartphone. However, if your child tries to use the app, a window will tell them that Swisscom Mobile Security has blocked it.
If your child subsequently installs more apps, these are automatically blocked by Application Control. Your child must then ask you to allow them to use such an app via Application Control.

4.7 Protection from unwanted calls and messages

The *Safe Contacts* function protects you from unwanted calls and messages. With *Safe Contacts* you can determine who you would like to receive calls and messages from, and block unwanted calls and spam messages.
You can choose the numbers you want to block. *Safe Contacts* blocks all incoming calls and text and picture messages from the selected numbers. Outgoing calls to the numbers on this list are also blocked (editable).

Using Safe Contacts

Safe Contacts blocks calls and messages from blocked numbers. Follow these instructions in order to block calls and messages from a new number:
1. Choose *Settings* from the main view. The list of settings is opened.
2. Select *Safe Contacts* from the settings list. NB: you will now need to enter your security code if you have not already done so.
3. Make sure that *Safe Contacts* is activated.
4. Select *Block numbers*. Enter your security code in order to block new numbers. The list of blocked numbers is opened.
5. Choose *Enter a number to block*.
6. Enter the name and, in the second field, the number you wish to block.
7. Select *Save* in order to add the number to the list of blocked numbers.

If *Safe Contacts* is activated, you will no longer receive calls or messages from the numbers on the list of blocked numbers (such calls will only be displayed briefly and will appear as unanswered in your calls list). All calls to the blocked numbers will also be barred.
If you want to treat the blocking of incoming and outgoing calls and messages differently, or turn it off, select the blocked contact from the list. In the window that then opens, you can delete the contact or make detailed changes.

Displaying blocked calls and messages
You can see which calls and messages have been blocked by *Safe Contacts*.
Follow these instructions to see which calls and messages have been blocked by *Safe Contacts:*
1. Select *Settings* from the main view. The list of settings is opened.
2. Select *Safe Contacts* from the settings list.
3. Choose *Show block history.*

5. Technical support

If you have any questions about installing, activating, deactivating or the free trial, call the Swisscom Hotline on 0800 55 64 64.

Our security partner's online support pages contain further information on the features of Mobile Security:
http://www.f-secure.com/support/

Please note, however, that your Swisscom Mobile Security software may differ slightly from the standard F-Secure product in terms of installation, activation, deactivation and appearance.