SecureMe v1.3.0
By Killer Mobile Software LLC
www.killermobile.com
info@killermobile.com

SecureMe is an Anti-Theft, Data Security & Protection application for SmartPhone devices. The application can automatically lock down, and prevent usage, send location details, hide, password protect or delete data you choose, either automatically on SIM change or remotely via SMS commands. You can even listen into the thief, get reports of calls made or sms's sent and much more. SecureMe runs completely hidden, is password protected and can optionally utilize uninstallation protection. SecureMe will satisfy all of your Mobile Security & Privacy needs!

BONUS! A special "Java" remote application is available for easy sending of the remote SMS commands!

******* You can purchase a license for continued use directly from www.killermobile.com *******

COMPATABILITY

All Series 60 (S60) 3rd & 5th Edition Devices are supported.

Nokia 3250, 5500, 5700, 6110, 6120, 6121, 6210, 6220, 6290, E50, E51, E60, E61, E61i, E62, E63, E65, E66, E70, E71, E75 E90, N69, N71, N73, N75, N76, N77, N78, N79, N80, N81, N81 8GB, N82, N85, N86, N91, N92, N93, N95, N95 8GB, N96, 5320 XM, 5320 XM, 5800 Xpress Music E52, E55, 5530 xpress, 6710 Navigator, 6730 Classic, N97, X6, Sony Ericson Satio, LG KS10, Samsung SGH-G810, Samsung INNOV8, Samsung SGH-L870

INSTALLING/UNINSTALLING

The application should be installed the same as all native Symbian applications. Transfer the application to your device via Bluetooth, USB, etc, or Download OTA and you will be prompted automatically to install the application.

* **NOTE:** Install to your internal device memory for optimum performance & stability. Save clips to your memory card.

To uninstall the application, go to the App. Manager (Typically Menu -> Settings - Data Mgr -> App Mgr), select Total Recall from the list, and choose **Options -> Remove**. This will uninstall the application completely.

** I**MPORTANT!** If you have enabled the "Protected" setting, you must disable this first, prior to being able to uninstall.

REGISTRATION

The application by default is in a 14 day trial mode state when first installed. Upon the first install you will be prompted to input your registration code, but during the 14 day demo period you will be able to bypass by choosing "Trial". You can input your registration at any time from the main Options menu.

IMPORTANT NOTE CONCERNING APPLICATION ACESSIBILITY
---

* Due to the nature of the application, access after the initial installation is only possible by dialing the password key, which by default is 5555, unless manually changed. No application icon will appear in your applications folder. Example: key in 5555 + press the green send key.

APPLICATION OPERATION

Main/Help Screen -

When you first install the application you will be presented with a language option for Hindi or English. This will choose which Alarm audio file is played in the event of a device lock down. This can

When you first run the application, you will see the About/Help screen. From this screen you have two options:

1) Options (left softkey) - This will have two sub-options:

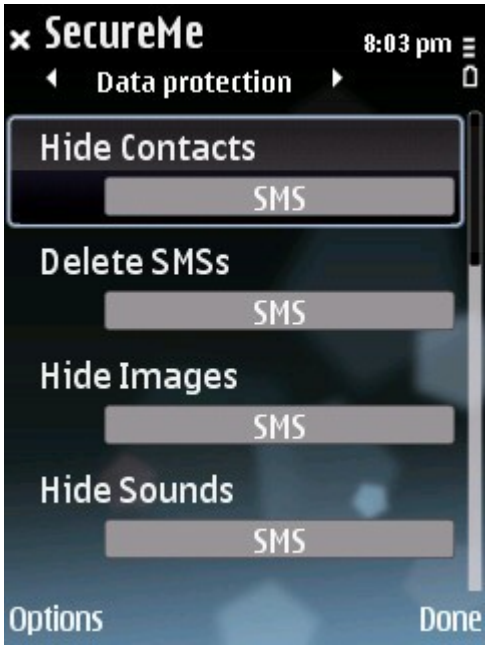
+ Register - to input your registration code if still in Trial mode
+ Exit - To shut down the application completely. Remember, the application will still restart on device reboot!

2) Hide - Hide will put the application in the background, but it will still be running.

Data Protection Settings Screen

** All Data will be automatically restored as soon as the proper SMS command is received, or the application is accessed successfully using the password.

- On SMS Command Receipt = The Data protection behavior will only take affect upon receiving an SMS command
- On SIM Change = The protection behavior will only take affect upon a SIM Change attack
- Always = the behavior will always be enabled



These settings can take affect automatically on SIM change, or via remote SMS command. Some can offer password protection at all times. Press the "Done" option to save the setting change(right softkey).

-) Hide Contacts - Options: On SMS Command Receipt, On SIM Change - Hides the contacts during a SIM Change Attack (Contacts will be restored upon exiting SIM Change Attack Mode)

-) Hide SMS's - Options: On SMS Command Receipt, On SIM Change - Hides SMS's during a SIM Change Attack

-) Hide Images - Options: On SMS Command Receipt, On SIM Change - Hides the Gallery Image files during a SIM Change Attack (Images will be restored upon exiting SIM Change Attack Mode)

-) Hide Sounds - Options: On SMS Command Receipt, On SIM Change - Hides the Gallery Sound files during a SIM Change Attack (Sounds will be restored upon exiting SIM Change Attack Mode)

-) Hide Videos - Options: On SMS Command Receipt, On SIM Change - Hides the Gallery Video files during a SIM Change Attack (Videos will be restored upon exiting SIM Change Attack Mode)

-) Hide Memory - Options: On SMS Command Receipt, On SIM Change - Hides the main Memory Card Contents during a SIM Change Attack (Memory will be restored upon exiting SIM Change Attack Mode)

-) Wipe Card - Options: On SMS Command Receipt, On SIM Change - Wipes the memory card

-) Clear Logs - Options: On SMS Command Receipt, On SIM Change - Deletes the call logs

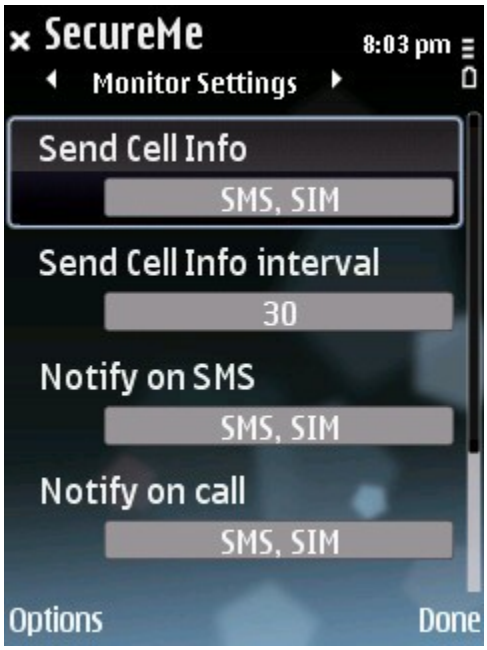
-) Lock screen and Keypad - Options: On SMS Command Receipt, On SIM Change - Locks the screen (places a canvas with a message "Protected by SecureMe" and locks all keys deeming the device unusable unless the proper password is inputted

-) Siren on lock screen - Options: Enabled/Disabled - plays the alarm audio file whenever the lock screen is active

-) Password Protect Contacts - Options: On SMS Command REceipt, On SIM Change, Always - Requires a password to enter the contacts application

-) Password Protect Messaging - Options: On SMS Command REceipt, On SIM Change, Always - Requires a password to enter the messaging application

---
Monitor Settings Screen



SMS = Upon receiving SMS command
SIM = Upon SIM change attack
All the time = All of the time

-) Send Cell/GPS Info - Options: SMS, SIM, All the time - Sends the Cell ID details to the Authorized numbers via SMS

-) Send cell/GPS info interval - In minutes - the interval at which the Cell ID is sent

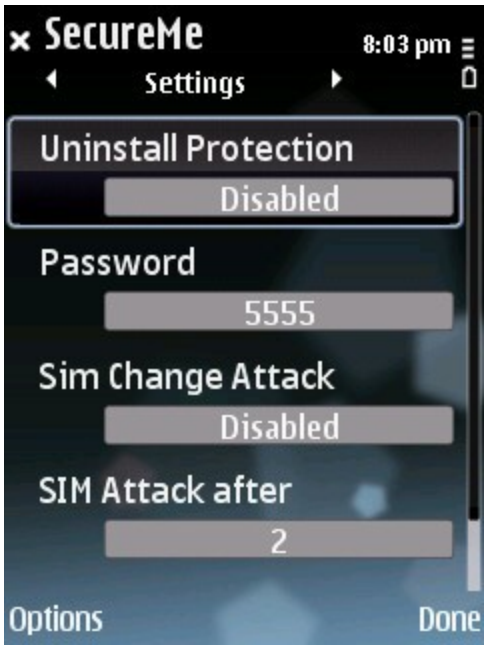
-) Notify on SMS - Options: SMS, SIM, All the time - Sends a copy of any sent/received SMS's to the Authorized numbers via SMS

-) Notify on Call - Options: SMS, SIM, All the time - Sends the call log details via SMS to the Authorized Numbers

-) Spy Call - Options: SMS, SIM, All the time - Application will automatically and silently answer the incoming call from the set Spy Number if enabled without

-) Call Me - Options: Enabled/Disabled - Application will respond to an SMS command by silently calling the number indicated in the SMS command

---
Main Settings Screen



-) Uninstall Protection - if enabled the application cannot be uninstalled unless this setting is disabled

-) Password - 4 digits - the password used for accessing the application

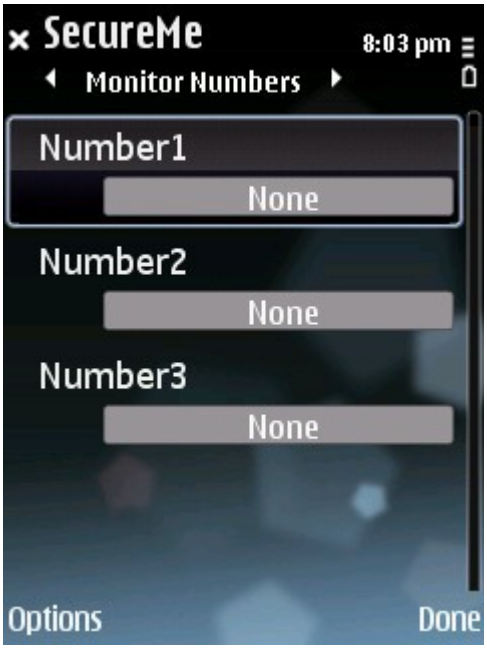
-) SIM Change Attack - Enabled/Disabled - If enabled upon SIM change to a SIM that is not on the authorized list the device will lock down automatically and the data protection settings will take affect per the settings

-) SIM Attack After - In Minutes - The delay after reboot until the SIM attack takes place

---

Authorized Number Screen

User can set up to three numbers that are used when sending Call logs, SMS's and Cell ID per the spy settings or the SIM Attack settings

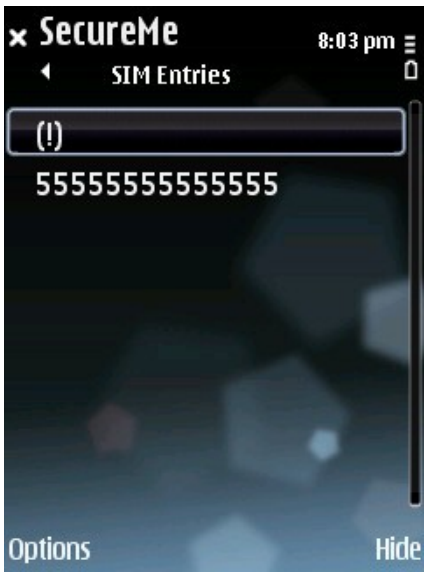


Spy Call Numbers Screen

Numbers that are used for the Spy Call setting (application will auto answer the call from these numbers silently if this setting is enabled or the application is in attack mode.

SIM Entries

By default, when you first install the application, the SIM you have inserted into the device will appear on the SIM Entries list. This SIM will NOT trigger a SIM attack, unless manually deleted. Also, any SIM that is present in the device when you input the password (ie 5555) will also be added to this "WHITELIST" and will not trigger a SIM Attack. The SIM number followed by the "!" sign indicates that this is the currently inserted SIM.



Options ->

1) Add SIM Number - Allows you to manually input a SIM number to the SIM Entries Whitelist

2) Edit SIM Number - Allows you to modify a SIM number that is already present on the list

3) Delete SIM Number - Allows you to delete a SIM Number present on the list

---

SMS Commands

SecureMe has various SMS commands that can be used for initiating an Attack Mode in case of loss or theft, deactivating an Attack Mode (and thus restoring certain data) and other useful features. The commands are listed below. ***A special Java "remote control" application is available, which is compatible with most devices that allows easy sending of the remote SMS commands.***

* ***NOTE:*** *Commands are NOT case sensitive*

* ***NOTE 2:*** *All SMS commands must be followed with your password, which is by default 5555. In the examples below the default password is referenced, if you changed your password please use this in place of "5555"*

* sm = the SMS prefix - the app will intercept all SMS's with a leading sm

sm start->send cell info pwd *** IF GPS coordinates are available, these are sent instead of Cell ID
sm stop->send cell info pwd
sm start->notify on sms pwd
sm stop->notify on sms pwd
sm start->notify on call pwd
sm stop->notify on call pwd
sm start->spy call pwd
sm stop->spy call pwd
sm start->call number pwd
sm stop->call pwd
sm start->spy all pwd
sm stop->spy all pwd
sm hide contacts pwd
sm restore contacts pwd
sm delete sms pwd
sm hide images pwd
sm restore images pwd
sm hide sounds pwd
sm restore sounds pwd
sm hide videos pwd
sm restore videos pwd
sm hide memory pwd
sm restore memory pwd
sm wipe card pwd
sm lock screen pwd
sm unlock screen pwd
sm start->protect contacts pwd
sm stop->protect contacts pwd
sm start->protect messaging pwd
sm stop->protect messaging pwd
sm start->all pwd
sm stop->all pwd

If you have any additional support queries, please contact us directly at info@killermobile.com or use the technical support form located at www.killermobile.com.

Copyright 2010 Killer Mobile Software LLC - All rights reserved