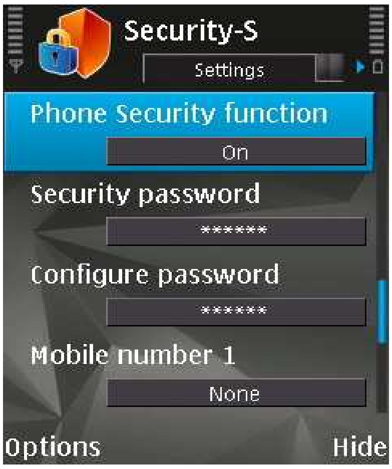
“Security 8.0” user manual



Phone Security function: On

Security password: ******

Configure password: ******

Mobile number 1: None

“**Security**” application is a value-added service on Nokia S60 3.0 platform. It can protect a mobile user from losing his/her phone just in case the phone is lost. For example, if a user has lost his /her phone and someone has picked up the phone. If another SIM card has plugged into in the phone, then a customized message will be automatically sent out to the pre-defined mobile numbers at the boot-up of the phone. In this case, the user can get to know the person’s mobile number.

In this release, the running of the app is very robust. Even if the app is terminated for some reasons, it will be automatically re-started, and keep it running. A user may use third party software to verify this function. Meanwhile, it can be set as non-uninstallable, which means a user may not uninstall the application if it is selected to be so.

This product has two kinds of registration:

- **Normal registration**
- **Special registration**

Once a special edition is registered, then the title of the application becomes “**Security-S**” rather than “**Security**”. For the special registration, a user may have the following additional **trace** function in addition to the one using the normal registration:

Once a user’s SIM card has been changed, and provided the “**Phone Security function**” is on, then a user (**“Mobile number1” or “Mobile number2”)** may send a short message to the current mobile number (can be obtained by the received SMS message) like “**123456:1**” or “**123456\1**” or “**123456/1**” (where “**123456**” is the “**Configure password**”, which is different from “**Security password**”) to turn on the trace function. Whenever, the person who picked up your phone makes outgoing calls, the callee’s personal information (name and number) will be sent to the number which enables the trace function. The format of the received SMS looks like:

Home: +86215438777 2007 may 25-15:39:44 call duration 5 min 4 seconds

if the person makes a call to his home. Sending “**123456:0**” or “**123456\0**” or “**123456/0**” will turn off the trace function (where “**123456**” is the “**Configure password**”).

A user may send command "123456:c" to configure the “**Phone number 1**”, where "123456" is the default configuration password. If the configuration password and the phone number are known to the person who wants to monitor another number, just simply send a message "123456:c" (“c” means configure) to make the current phone number to be set as "**Phone number 1**" in the "**Settings**".

For those users, who have not registered the special version of the software, the user has only one day trial as long as the product is not expired (3 days and some limited number of usage). During the trial period of time, the “**Configure password”** cannot be changed**.**

When “**Security**” is sending SMS, there is no outgoing signing shown on the top-right corner of the screen, and when “**Security**” is receiving a configuration SMS, there is no indication of receiving a message (like the sound or a dialog shown on the screen).

The purpose of having two separate passwords is to prevent the “**Security password**” from being seen when a configuration SMS is not deleted immediately if “**Security password**” is the same as “**Configure password**”. “**Configure password**” is only used for SMS configuration purpose ONLY.

For security reason, the application can **ONLY** be auto-started at the machine boot-up. Once the application is installed, a user cannot find it anywhere in the “**My Own**” or “**Installed**” folders. The main reason for this is that it prevents the phone-picker from un-installing the application and/or finding the existence of the application on the phone if the phone is lost.

How to enter to application user interface:

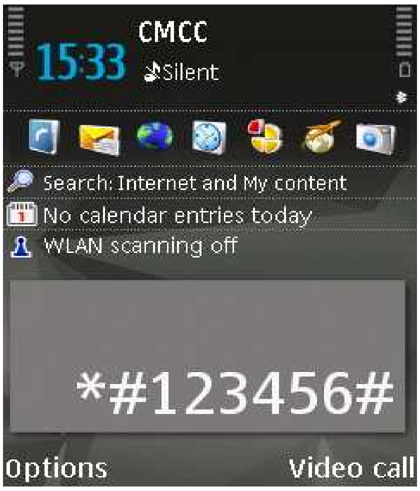
For security reason, the application can **ONLY** be auto-started at the machine boot-up. Once the application is installed, a user cannot find it anywhere in the “**My Own**” or “**Installed**” folders. The main reason for this is that it prevents the phone-picker from un-installing the application and/or finding the existence of the application on the phone if the phone is lost.

In order to enter the application, a user has to “**dial**” a “**Security Password**” (which is defined by the application) to make the application appear. The number is something as follows:

123456#

where “**123456**” is the default “**Security password**”, which is defined in the “**Settings**”. Once the password is changed, it has to be changed as well. It works like the way as how to get the IMEI number of the phone. The comparison of the passwords is only compared with the latest few digits. For example, the input “***#123456#**” could be also right to bring the “**Security**” application to the front!

Once the user has entered the application, the user has the freedom to change the password to any other ones (which consists of numeric numbers from “**0**” to “**9**”). Then length of the password should be no less than **6**, and the maximum length is **10**.



How to make a telephony call recording:

If there is an established call, simply press “*****” key; release the key “*****”; then press “**9**” key, it will start the recording over the telephony line. Another repeat of the above key combination (“*****” + “**9**”) will stop the recording process. If a user wants to record it again, then the user just needs to press the key combination again will start telephony recording again and so on. All of the data recorded during a call session will be saved into one single file. A user may check the file in the “**Audios**” window of “**Security**” or from the S60 “**Media gallery**”.

For some of the phones, which have the camera key, a user may also use the **camera key** to do the telephony recording. One press will trigger the call recording, and another **camera key** press will stop the recording. Press the key again, it will trigger recording again.

The recorded file name will start with the telephone number, and its extension name is "amr".

Application protection function:

"**Security**" also provides a very important function lock some specific applications to protect those applications from being accessed by some people. More information can be found in the following section:

Note: "**Security**" application does not support Nokia PC suite backup function!

1. Settings

1) Camera key to record

When it is on, after a call has been established, a user is able to use the "**Camera key**" to start to record a telephony. When it is "off", pressing "**Camera key**" will not do anything.

2) Autolock function

When it is on, during a predefined period of time, if keyboard is not touched, then keyboard will automatically be locked.

3) AutoLock time interval

Define the time interval for activating the key lock.

4) Power on function

When this option is on, then an alarm will be set automatically every day according to the days defined in "**Power on days**"
Please be noted that the setting in this "**Security**" application will override the time set in the S60 "**Clock**" application (if it has any alarm set there). However, if a user goes to the S60 "**Clock**" to set alarm again, then it will override this setting.

5) Power on days

Define the days to be alarmed for the week.

6) Power on time

Define the alarm time for the days defined in "**Power on days**".

7) Shut down function

When this function is on, the mobile phone will be turned off automatically at the time defined in "**Shut down a**t" every day.

When this option is off, then it has no effect at all.

8) Phone security function

If this option is on, then a SIM card change event will trigger the sending of SMS to the specific mobile numbers.
If this option is off, then even a SIM card change event happens, nothing will be done.

9) **Security password**

This is used to set the phone security password. The default password is "**123456**". A user may "**dial**" this number in the active idle screen to bring the app to the foreground. Please be noted that the application can ONLY be started at boot-up.

If a user has changed the password to something else, then the user needs to "**dial**" the new password in order to get into the application. For example, if a user has changed the password to "**456789**", then in order to bring forward the application, a user has to "**dial**":

456789#

Whenever there is a prompt for inputting a password to make a field change, then this password should be used.

10) **Mobile number1**

This is the mobile number used to send SMS to if there is SIM card change event happens and **"Phone security function**" is on. At each boot-up, a customized SMS message is sent to this number once only. In the next boot-up of the phone, the SMS will be sent again until the number of sent SMS has reached to the pre-defined maximum number of SMS. **Please be noted that this number should be a mobile number**.

11) **Mobile number 2**

It works the same way as last item.

12) **Phone security message**

Define the customized SMS for sending to "**Mobile number 1**" and "**Mobile number 2**". The message length should not be longer than 140 characters.

13) **Max number of SMS**

Define the maximum number of SMS to be sent to "**Mobile number 1**" and "**Mobile number 2**". If a user has defined two valid mobile numbers in the number fields, then each of the number will receive half of this maximum number of SMS if a SIM card event happens.

Please be noted: if the product is not registered, then "**Security**" can ONLY allow maximum of **2** SMS messages regardless of the setting in this field.

14) **Fake trigger type**: define the way to trigger a fake call. It is very useful in a situation when a user wants to make an excuse to go away. This function emulates an incoming call from someone though there is no call at all. Make sure there is a selected ring tone selected to make the function properly. Once the function is activated, a user may see a flashing phone icon shown on the top left corner of the screen, indicating there is a pending faked call on-going.

- **None**: the function is disabled
- **By Hotkey**: a user may press "**Fake call key sequence**". Once the key sequence is pressed on any of the screen, after "**Fake time delay"** times out, a faked incoming call will happen.

  For **QWERTY** layout keyboard, a user may press "**Ctrl**" + "**S"** at the same time to activate the fake call emulation.
- **By time**: a faked call will happen at a specific time defined by "**Fake trigger date"** and **"Fake trigger time"**.

15) **Fake call key sequence:** when "**By Hotkey"** is selected for the "**Fake Trigger Type**", pressing the key sequence will trigger a "**Fake time delay**", then followed by a fake call.

16) **Fake caller's name**: the caller's name appearing in the incoming call. If it is null, then, the "**Fake phone number**" is displayed instead.

17) **Fake time delay**: define the time delay for triggering the incoming call after a user presses the hot key defined by "**Fake call key sequence"**. This item only appears when "**Fake trigger type"** is set to "**By Hotkey".**

18) **Fake phone number**: when "**Fake caller's name**" is null, then this number appears in the faked incoming call.

19) **Fake ring tone**: define the ring tone to be used in the faked call.

20) **Fake trigger date**: define the date for triggering the fake call. This item only appears when "**Fake trigger type"** is set to "**By time".**

21) **Fake trigger time**: define the exact time on the day for triggering the fake call. This item only appears when "**Fake trigger type"** is set to "**By time".** At the time, a faked incoming call will happen.

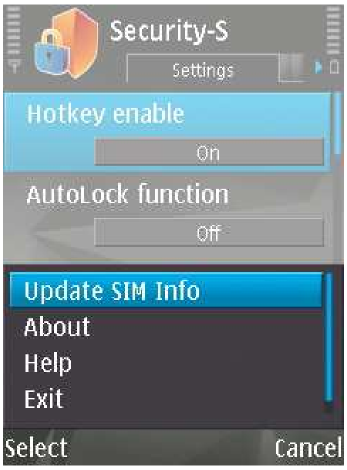
22) **Auto start enable**

By default, this application is auto-started, and this is the ONLY way to get the app started. If a user turned this option to off, then this application will never have a chance to start it again unless the user re-install the application.

23) **Enable uninstallation**

If this flag is ON, this is application is able to be uninstalled by S60 application manager. However, if this flag is off, the application is not allowed to be uninstalled.
A user has to use to this function carefully. If it is set off, the application is even not allowed to be re-installed (which involves an un-installation process).

Menu functions



1) **Update SIM info**

If a user has changed a new SIM card, and the user does not want to receive the annoying SMS due to the change event, then the user need to select this menu item to update the SIM card information. As such, no SMS messages will be fired!
If a product has not been registered, then a user may have 5 times to make the selection successful.

2) **Edit**

This menu only appears when the current item in the list box is “**Mobile number 1**” or “**Mobile number 2**”. It is used to set the mobile numbers for sending SMS messages when SIM card is changed. When there is no contact item in the phonebook, a user may use this to set the numbers. Please be noted the numbers should be mobile numbers!

3) **Register**

This is used to register the product. After the application has been registered, this item will not be shown any more. When the user firstly starts the application, the user has:

- 3 days trial or
- 6 free SIM card info updates
- 2 free sending SMS
- 10 free phone shutdown
- 10 free phone alarm sets
- 10 free key locks
- 10 free normal key recording
- 10 telephony audio recording
- 10 screen captures

After the product has expired, a user has to purchase a pincode to register this product.

4) **About**

Get the more detailed information about the product. It shows where to register the product!

5) **Help**

Invoke help function

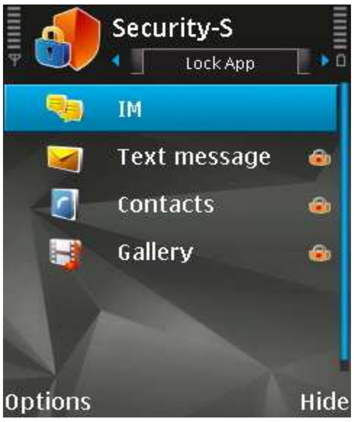
6) **Exit**

Exit the application.

7) **Hide**

Push the application to the background, and the application is running at the background.

2. Lock applications



This window is used to manage some lock applications.

A user may select any of the applications to be locked. As such, once the application is selected to be locked, the application cannot be launched unless it is set to be unlocked. For example, if an application called “**Messaing**” is selected to be locked, the application cannot be launched in any ways. A locked application is shown in the window with a “**Lock**” icon. Only after a user enters “Security” again to make it inactive by clicking the pressing “**OK**” key, the application becomes accessible again.

Menu functions:

Add Lock App: select an application to add into the lock application list. Once the application is selected, it is made active by default.

Activate: make the current item lock active

Cancel: make the current item lock inactive

Activate all: make all of the applications in the window lock active

Cancel all: make all of the applications in the window lock inactive

Delete: delete the current application from the lock application list

Help: launch the help function

Exit: Exit the application

3. Audios

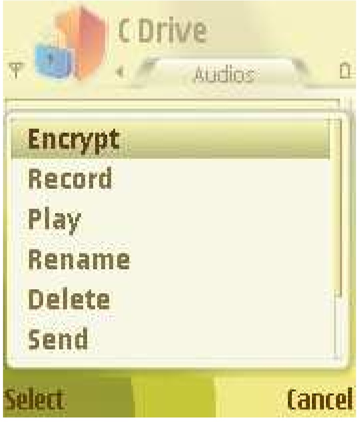
This window is used to view the recorded telephony audio messages during an established call, or after a user has pressed the “**Normal audio recording**”

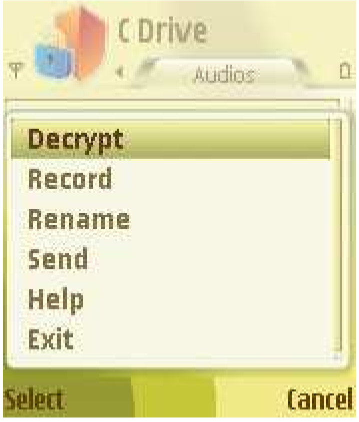
This window also provides the function for **encrypting/decrypting** the files to protect the personal privacy. The encrypted file has a “**+**” suffix at the end of the file name, while the decrypted file name should be the one without “**+**”. Should the file name exist, then the user is prompted for a new name for the output.

When encrypting, a user needs to supply a password to encrypt the file. The password is the one defined in “**Security Password**” in “**Settings**”. When decrypting, a user has to supply a correct password to decrypt it since this is a protected function. During the decrypting process, if the password used to encrypt the file before is different from the current “**Security Password**”, then a user has to enter the previous password correctly to decrypt the file.

The default file folder is the one defined in the S60 “**Recorder**” application. If phone memory is selected in the “**Settings**” there, then the default folder is for phone memory. In order to view the other memory location, a user has to select using the menu item.

Menu functions





Menu functions:

Encrypt: encrypt the current file in the list box.

Decrypt: decrypt the current file in the list box.

Record: record a file. When recording, a red-dot will keep blinking at the top-left corner of the screen.

Stop: stop the current recording. A user may also the “**Normal audio recording”** key to stop the recording.

Play: play the current audio file.

Rename: rename the current audio file

Delete: delete the current audio file.

Send: send the current audio file.

Show E drive: Show the audio files in memory card.

Show C drive: Show the audio files in the phone memory.

Exit: Exit the application