

F-Secure Mobile Security™ for Nokia E51, E71 and E75

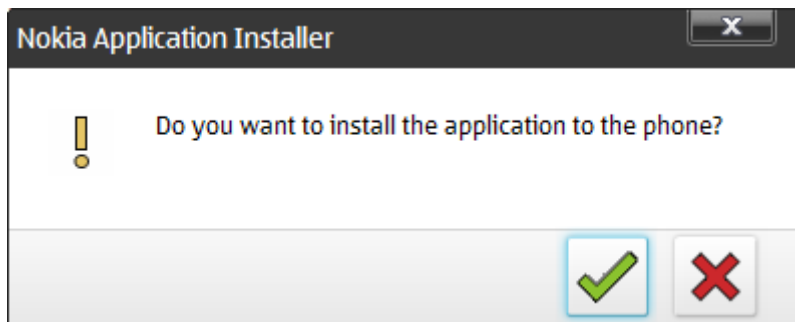
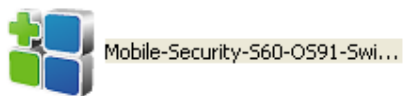
1 Installing and Activating F-Secure Client 5.1

N.B.: The previous version of F-Secure Mobile Security does not have to be uninstalled. The new version will use your existing subscription, if you have one.

Installation:

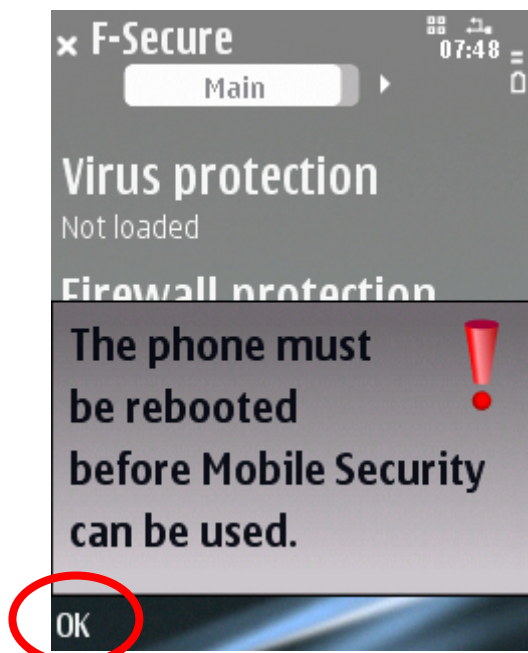
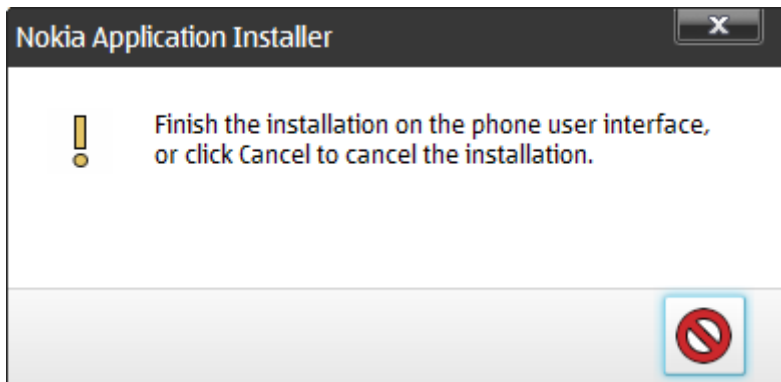
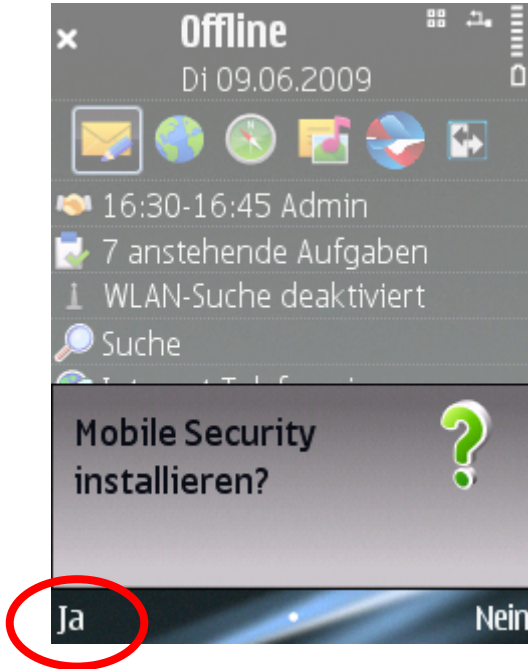
Download the installation file to your computer and transfer it to the device
or download the installation file to your computer and install the product via the Nokia PC suite
or download the installation file directly to your device.

Installation will start.





swisscom

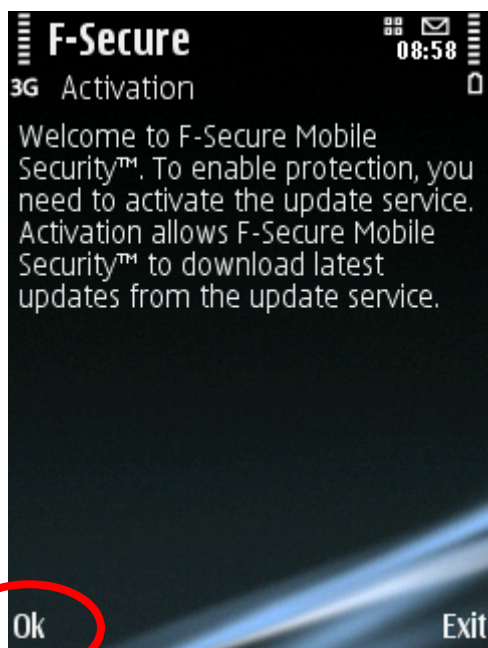


Once installation is complete, reboot the device if you are asked to do so.

Once installation is complete you have to activate the product. The product does not protect your device until you have activated it.

Activation

1.1 To start activation:

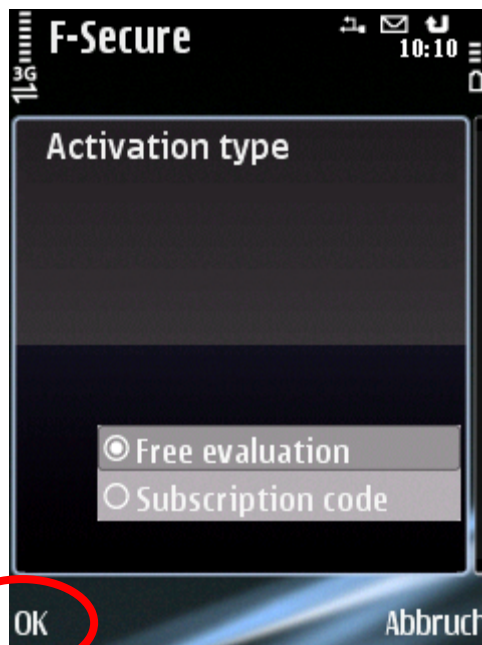
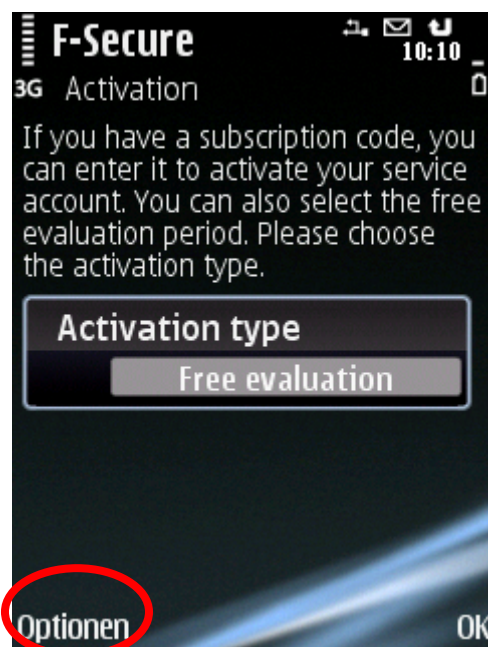


1. Open the application. The welcome screen will be displayed.

2. Press OK.

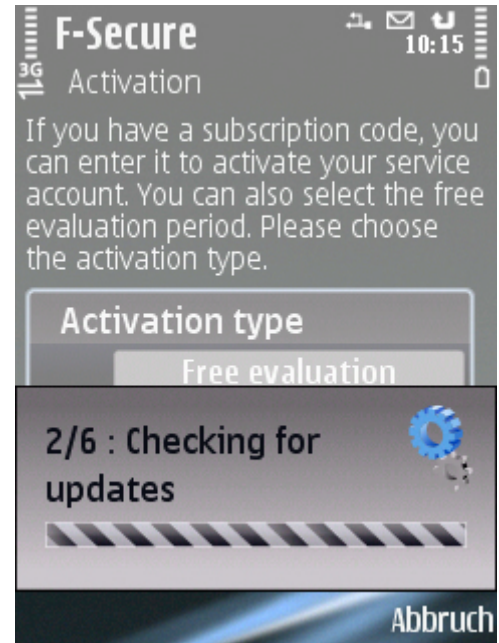
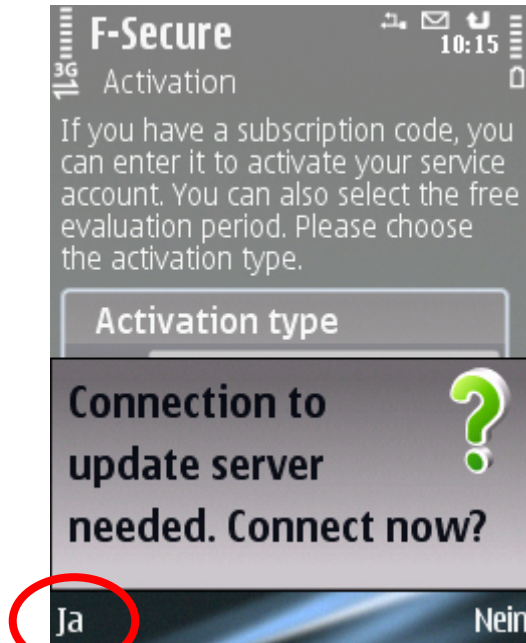
3. Select the activation type: To begin the evaluation period, select the activation type **Free evaluation**, if it is available, and click on OK

or • If you wish to have the fully licensed version, select the activation type **Subscription code** and click on **OK**. Enter your subscription code and click on **OK**.

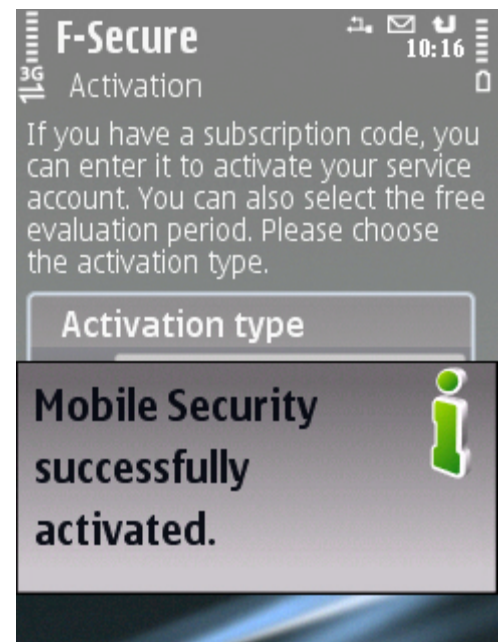
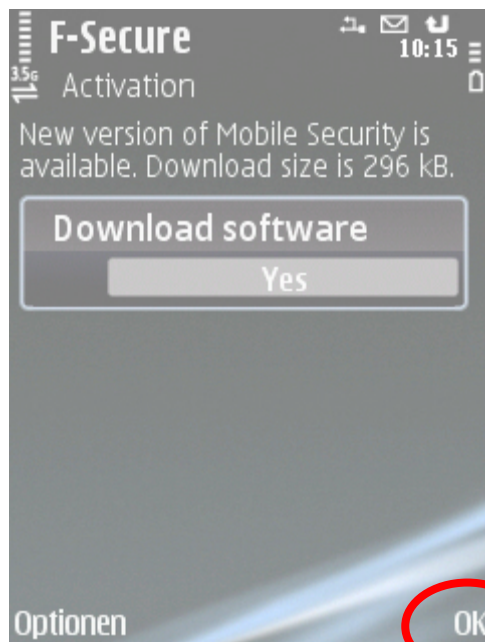




swisscom



4. Click on **Yes** and select the Internet access point to connect to the update server and begin to download the updates. The application will connect to the update server and submit your subscription code. During the first update the application downloads the latest virus definition databank.



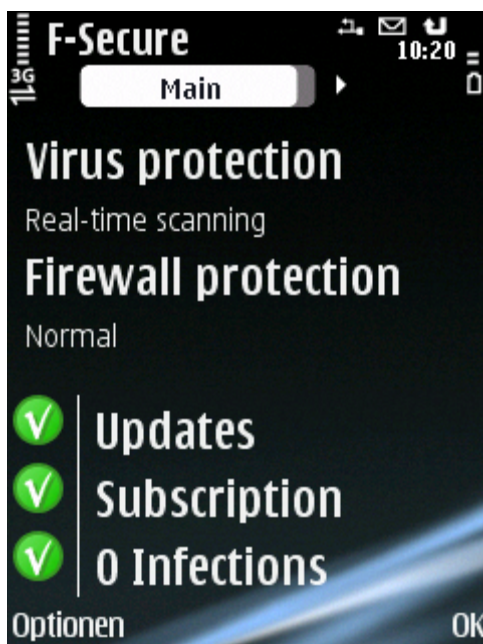
5. As soon as the download is complete you will receive a message telling you that registration was successful and the application activated. Click on **OK** to complete activation. Once activation is complete the download may also want to update the software.



swisscom

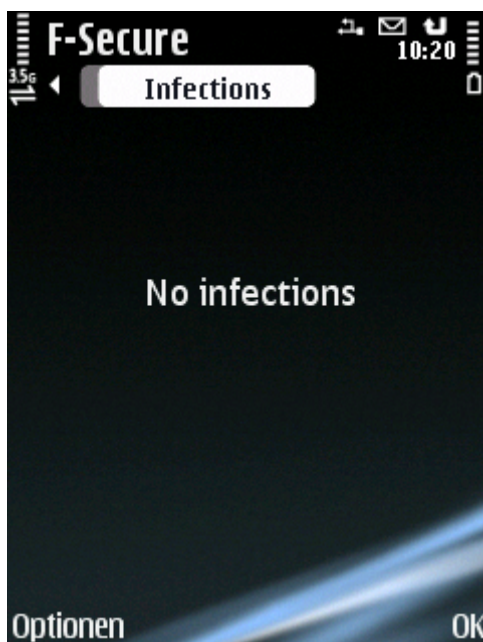
6. Once you have activated the application, scan your device for viruses to ensure that it is clean. You will find further information about this in the section “Scanning for Viruses” below. You should scan your device whenever you are asked to do so by the application.

2 Scanning for Viruses



F-Secure Mobile Security runs in the background and scans your files automatically.

1. Mobile Security alerts you if a virus is found during real-time scanning. Click on **Yes** to display the infected file or files or on **No** to close the display.



2. The “Infections” view displays a list of the infected files detected on your device as well as the status of that file (under quarantine, released). If you want to view more details about an infected file, follow these instructions:

1. Scroll to the infected file and select this file.

2. Select **Show**.

3. The Infection details view displays the path and file name of the infected file, and the name of the virus that has infected the file.



swisscom

2.1 Processing Infected Files

To process infected files, follow these instructions:

1. In the “Infections” view scroll to the infected file that you would like to process.
2. Select the file.
3. Select one of the following commands:
 - **Delete** – deletes the infected file. This is the recommended option. The file will be completely removed from your device.
 - **Quarantine** – Places the infected file under quarantine if the file is not yet quarantined. A quarantined file is locked and cannot harm your device when F-Secure Mobile Security is on.
 - **Release** – Releases the quarantined file. If you release a file, it is not locked any more. You access it at your own risk.



swisscom

3 Protecting Confidential Information

Theft protection ensures that your device or saved data cannot be used if your device is stolen.

3.1 Locking the device

Theft protection can lock your device automatically when the SIM card is replaced. The locked device can only be released using a security code. **To lock the device, follow these instructions:**

1. Browse to **Settings** and select.
2. Select the option **Theft Protection**.
3. Enter a **security code**. The security code must contain at least 5 characters. Keep the code in a safe place.
4. To lock your device, when you replace the SIM card select the option **Yes** under **Lock when replacing SIM card**.

3.2 Using Remote Theft Protection

To lock your device or delete all information on it you can send a text message with your security code to the device. **To set up remote theft protection, follow these instructions:**

1. Browse to Settings and click on the select button.
2. Select the option **Theft Protection** under Settings.
3. To lock the device remotely, follow these instructions:
 - a. Enter a security code if you have not already created one.
 - b. Activate **Remote security**. The locked device can only be released with your security code.
4. To reset the device remotely, follow these instructions:
 - a. Enter a **reset code**. The reset code must contain at least 8 characters. Keep the code in a safe place.
 - b. Activate **Remote resetting**. When the device is reset, all data saved on it will be removed.

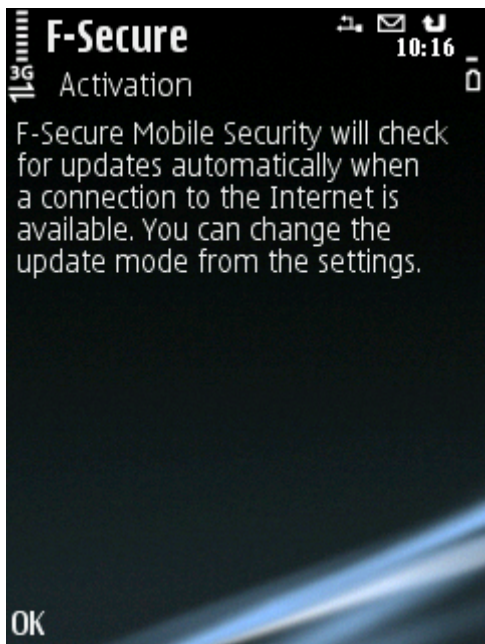
To lock or reset the device remotely, follow these instructions:

To lock the device, send the following text message to your device:
#LOCK#<security code> (e.g.: #LOCK#abcd1234)

To delete data from your device, send the following text message to your device:
#WIPE#<reset code> (e.g.: #WIPE#abcd1234). Because memory cards can be removed slightly, you should store all confidential information in the device memory, which you can then lock and delete using the theft protection function. The security code protects the theft protection settings. You must enter your most recent security code before you can make changes to the theft protection settings.

4 Keeping the Product Up to Date

4.1 Automatic Updates



F-Secure Mobile Security includes an automatic update service, which regularly updates the virus definition data bank in the application. Only an up-to-date virus definition database protects your device against the latest viruses. Automatic updates are in use after you have activated the product. The application requires an active Internet connection for the updates. When a connection to the Internet is available, the application checks when the virus definition database was last updated and downloads new updates if necessary.

4.2 Manual Updates

You can also update the application manually:

1. Browse to **Virus protection** and click on the select button.
2. Select **Update now**.
3. Select the internet access point to connect to the update server. The application downloads the latest virus definition database and puts it into use immediately.
4. When the update is complete, click on **Yes** to check your device for viruses when you are prompted to do so. You will find further information about this in the section "Scanning for Viruses".

Version Updates When a new F-Secure Mobile Security version is available, a message asks you to download it. The application restarts automatically when the update is completed.

4.3 Technical Support

Further information is available in the F-Secure Mobile Security Anti-Virus for S60 User's Guide (in English only) which can be downloaded from <http://mobile.f-secure.com/>. If you have questions about F-Secure Mobile Security not covered in the manual or online services at <http://www.F-Secure.com/>, you can contact your local F-Secure distributor or F-Secure Corporation directly.