

F-Secure Mobile Security™ for S60

1. Installation und Aktivierung

Zurück Version Die vorherige Version von F-Secure Mobile Anti-Virus muss nicht deinstalliert werden. Überprüfen Sie im Anschluss an die Installation der neuen Version die Einstellungen von F-Secure Mobile Security.

Installation **So installieren Sie die Anwendung:**

- Laden Sie die Installationsdatei auf Ihren Computer herunter und verschieben Sie sie auf das Gerät.
- Laden Sie die Installationsdatei auf Ihren Computer herunter und installieren Sie das Produkt über Nokia PC Suite. Oder:
- Laden Sie die Installation direkt auf Ihr Gerät herunter. Die Installation startet automatisch.

Starten Sie das Gerät nach der Installation neu, falls das Installationsprogramm Sie dazu auffordert. Nachdem die Installation abgeschlossen ist, müssen Sie das Produkt aktivieren. Erst mit der Aktivierung schützt das Produkt Ihr Gerät.

Aktivierung **So aktivieren Sie die Anwendung:**

1. Starten Sie die Anwendung. Der Willkommensbildschirm wird angezeigt.
2. Drücken Sie auf **Fortfahren**.
3. Wählen Sie den Aktivierungstyp aus:
 - Um das Produkt nur mit aktivierter Diebstahlsicherung zu aktivieren, wählen Sie als Aktivierungstyp **Nur Diebstahlsicherung** und drücken Sie anschließend **Fortfahren**.
 - Um die lizenzierte Vollversion zu erhalten, wählen Sie **Anmeldenummer** als Aktivierungstyp und drücken Sie anschließend **Fortfahren**. Geben Sie Ihre Anmeldenummer ein und drücken Sie **OK**.
4. Drücken Sie **Ja** und wählen Sie den Internet-Zugriffspunkt, um eine Verbindung mit dem Update-Dienst herzustellen und mit dem Herunterladen der Updates zu beginnen.

Die Anwendung baut nun eine Verbindung zum Update-Dienst auf und übermittelt Ihre Anmeldenummer. Während des ersten Updates lädt die Anwendung die aktuelle Virendefinitionsdatenbank herunter.
5. Nachdem das Produkt alle erforderlichen Updates heruntergeladen hat, ist die Anwendung vollständig. Drücken Sie **Fortfahren**, um die Aktivierung zu beenden.

Scannen Sie Ihr Gerät nach Viren, nachdem Sie die Aktivierung beendet haben, um sicherzustellen, dass Ihr Gerät virenfrei ist. Weitere Informationen hierzu finden Sie im Abschnitt **Scannen nach Viren** weiter unten.



Sie sollten Ihr Gerät immer dann scannen, wenn Sie von der Anwendung dazu aufgefordert werden.

2. Scannen nach Viren

F-Secure Mobile Security wird im Hintergrund ausgeführt und scannt Ihre Dateien automatisch.

1. Sie werden von F-Secure Mobile Security benachrichtigt, wenn bei einem Echtzeitscan ein Virus entdeckt wird. Drücken Sie **Ja**, um infizierte Dateien sofort anzuzeigen oder **Nein**, um sie später anzuzeigen.
2. Die Ansicht „Infektionen“ enthält eine Liste der infizierten Dateien auf dem Gerät sowie den Status der Datei (entweder unter Quarantäne gestellt oder freigegeben).

So zeigen Sie weitere Informationen über eine infizierte Datei an:

1. Blättern Sie zur infizierten Datei und drücken Sie die Auswahl Taste.
2. Wählen Sie **Anzeigen** aus.
3. In der Ansicht „Infektionsdetails“ werden der Pfad und der Name der infizierten Datei sowie der Name des verursachenden Virus angezeigt.

Verarbeitung infizierter Dateien

So verarbeiten Sie infizierte Dateien:

1. Blättern Sie in der Ansicht „Infektionen“ zur infizierten Datei, die Sie verarbeiten möchten.
2. Drücken Sie die Auswahl Taste.
3. Sie haben nun folgende Optionen:
 - **Löschen** – löscht die infizierte Datei. Dies ist die empfohlene Option. Die Datei wird vollständig von Ihrem Gerät entfernt.
 - **Quarantäne** - verschiebt die infizierte Datei in die Quarantäne, falls dies noch nicht geschehen ist. Eine Datei unter Quarantäne ist gesperrt und kann Ihr Gerät nicht schädigen, solange F-Secure Mobile Security aktiviert ist.
 - **Freigeben** – gibt die unter Quarantäne stehende Datei frei. Wenn Sie eine Datei freigeben, ist sie nicht länger gesperrt. Der Zugriff geschieht auf Ihr eigenes Risiko.

3. Verhindern von unbefugtem Netzwerkdatenverkehr

Die Firewall von F-Secure Mobile Security arbeitet unauffällig im Hintergrund. Sie überwacht sowohl den ein- als auch den ausgehenden Internet- und Netzwerkverkehr und schützt Sie vor Eindringversuchen. Über vordefinierte Firewall-Schutzstufen können Sie eine Ihren Anforderungen entsprechende Schutzstufe einstellen.

Auswahl der Sicherheitsstufe

So wählen Sie die Sicherheitsstufe aus:

1. Navigieren Sie zu **Einstellungen** und drücken Sie die Auswahl Taste.
2. Wählen Sie in der Einstellungsauswahlliste **Firewall** aus.
3. Wählen Sie die gewünschte Sicherheitsstufe aus:
 - **Alle ablehnen** – blockiert den gesamten Netzwerkdatenverkehr.
 - **Hoch** – lässt die meisten gängigen Anwendungen zu und blockiert jeglichen eingehenden Datenverkehr.
 - **Normal** – lässt alle ausgehenden Verbindungen zu und blockiert jeglichen eingehenden Datenverkehr.
 - **Alle zulassen** – lässt jeden Netzwerkdatenverkehr zu.
 - **Benutzerdefiniert** – Mit dieser Option wird Datenverkehr im Netzwerk basierend auf den von Ihnen definierten Regeln zugelassen. Haben Sie die Firewall-Stufe **Benutzerdefiniert** aktiviert, können Sie Ihre benutzerdefinierten Regeln bearbeiten. Klicken Sie hierzu auf **Optionen > Benutzerdefinierte Regeln bearbeiten**.

4. Schutz vertraulicher Daten

Anti-Theft verhindert, dass Ihr Gerät und die auf ihm gespeicherten Daten nach einem Diebstahl missbraucht werden.



Da Speicherkarten mühelos entfernt werden können, speichern Sie Ihre vertraulichen Informationen in den Gerätespeicher. Diesen können Sie sperren und mit Anti-Theft zurücksetzen.

Verwenden der Gerätesperre

Anti-Theft kann Ihr Gerät automatisch sperren, wenn die SIM-Karte im Gerät geändert wurde. Das gesperrte Gerät lässt sich nur mit Ihrem Sperrcode entsperren.

So richten Sie die Gerätesperre ein:

1. Browsen Sie zu **Einstellungen** und drücken Sie die Auswahl Taste.
2. Wählen Sie in der Einstellungsauswahlliste **Anti-Theft** aus.
3. Geben Sie einen **Sperrcode** ein. Der Sperrcode muss aus mindestens 5 Zeichen bestehen. Bewahren Sie ihn an einem sicheren Ort auf.



Ihr Sperrcode sichert die Anti-Theft-einstellungen. Um Anti-Theft-einstellungen zu ändern, müssen Sie Ihren aktuellen Sperrcode eingeben.

4. Wenn Sie möchten, dass Ihr Gerät gesperrt wird, wenn die SIM-Karte gewechselt wird, wählen Sie unter **Nach Wechseln der SIM-Karte sperren** die Option **Ja** aus.

Verwenden der Remote-Anti-Theft

Mithilfe der Remote-Anti-Theft können Sie an Ihr Gerät eine SMS-Textnachricht mit Ihrem Sperrcode senden, um dessen Standort zu bestimmen oder um es zu sperren. Außerdem können Sie einen Sicherheitscode an Ihr Gerät senden, um alle auf Ihrem Gerät vorhandenen Informationen zu löschen.

So richten Sie die Remotesperre ein:

1. Browsen Sie zu **Einstellungen** und drücken Sie die Auswahl Taste.
2. Wählen Sie in der Einstellungsauswahlliste **Anti-Theft** aus.
3. Wenn Sie in der Lage sein möchten, Ihr Gerät remote zu sperren, befolgen Sie diese Anweisungen:
 - a. Geben Sie einen **Sperrcode** ein, wenn Sie noch keinen erstellt haben.
 - b. Aktivieren Sie die **Remotesperre**.

Das gesperrte Gerät lässt sich nur mit Ihrem Sperrcode entsperren.

4. Wenn Sie in der Lage sein möchten, Ihr Gerät remote zu reinitialisieren, befolgen Sie diese Anweisungen:
 - a. Geben Sie einen **Reinitialisierungscode** ein. Der Reinitialisierungscode muss aus mindestens 8 Zeichen bestehen. Bewahren Sie ihn an einem sicheren Ort auf.
 - b. Aktivieren Sie die **Reinitialisierung**.

Bei einer Reinitialisierung werden alle auf dem Gerät gespeicherten Daten gelöscht.

So sperren oder reinitialisieren Sie Ihr Gerät remote:

Senden Sie die folgende SMS-Textnachricht an Ihr Gerät.

- Um das Gerät zu sperren, senden Sie folgende SMS:
#LOCK#<Sperrcode> (z. B. #LOCK#abcd1234)
- Um das Gerät zu reinitialisieren, senden Sie folgende SMS:
#WIPE#<Reinitialisierungscode> (z. B. #WIPE#abcd1234)
- Um den Standort des Geräts zu ermitteln, senden Sie folgende SMS:
#LOCATE#< Sperrcode> (For example: #LOCATE#abcd1234)



Anti-Theft speichert keine Standortdaten. Die einzige Standortinformation befindet sich in der SMS, die an Sie gesendet wird.

5. Sicherheit beim Internetsurfen

Der Browsing-Schutz bietet Sicherheit vor Websites, die Ihre persönlichen Informationen wie Kreditkartennummern, Benutzerkontoinformationen und Kennwörter stehlen können.

Der Browsing-Schutz überprüft Websites, zu denen Sie über den Standardbrowser Ihres Geräts navigieren. Wenn Sie einen Browser eines Drittanbieters verwenden, bietet Ihnen der Browsing-Schutz keine Sicherheit beim Internetsurfen.



Schalten Sie den Webbrowser aus und löschen Sie dessen Speicher, bevor Sie den Browsing-Schutz zum ersten Mal verwenden.

So aktivieren Sie den Browsing-Schutz:

1. Navigieren Sie zu **Einstellungen** und drücken Sie die Auswahl Taste.
2. Wählen Sie in der Einstellungsauswahlliste **Browsing-Schutz** aus.
3. Aktivieren Sie **Browsing-Schutz**.
4. Wählen Sie unter **Zu verwendendes Netzwerk** aus, ob der Browsing-Schutz immer oder nur dann aktiv sein soll, wenn Sie über das Mobilfunknetz Ihres Netzbetreibers im Internet surfen:
 - Wählen Sie **Nur mein Betreiber**, um den Browsing-Schutz nur dann zu verwenden, wenn Sie das Netzwerk Ihres Mobilfunkanbieters verwenden.
 - Wählen Sie die Einstellung **Alle Betreiber**, damit der Browsing-Schutz auch aktiviert bleibt, wenn Sie unterwegs sind oder sich außerhalb des Netzwerks Ihres Mobilfunkanbieter befinden.

Datenschutzmodus

Um die Servicequalität aufrechtzuerhalten, kann der Browsing-Schutz Informationen über Websites, die schädliche Inhalte aufweisen, automatisch zur Analyse senden. Sie können festlegen, welche Informationen zur Analyse gesendet werden sollen.

So ändern Sie die Datenschutzmodus:

1. Navigieren Sie zu **Einstellungen** und drücken Sie die Auswahl Taste.
2. Wählen Sie in der Einstellungsauswahlliste **Andere Einstellungen** aus.
3. Wählen Sie im Datenschutzmodus
 - die Option **Nur Statistiken** aus, um nur Browsing-Schutzstatistiken und die Serververbindungsdaten zu senden.
 - die Option **Alle zulassen** aus, Statistiken und Informationen auf Websites zu senden, die noch nicht analysiert wurden oder schädliche Inhalte aufweisen.



*Für optimale Servicequalität empfehlen wir Ihnen, für den Datenschutzmodus die Einstellung **Alle zulassen** zu verwenden.*

Datenschutz-erklärung

Durch das Senden von Informationen wird Ihr Datenschutz nicht gefährdet.

Auch wenn die gesendeten Informationen in einigen Rechtsgebieten als persönlich eingestuft werden können, ist Ihr Datenschutz während des Vorgangs sichergestellt. Wir übertragen die Informationen gesichert, entfernen nicht benötigte persönliche Informationen und verarbeiten die Informationen anonym und nicht personenbezogen. Dadurch kann zwischen den Informationen und Ihnen keinerlei Bezug hergestellt werden. In den gesendeten Informationen sind keine Kontoinformationen, IP-Adressinformationen oder Lizenzinformationen enthalten. Darüber hinaus wird Ihr Datenschutz durch eine verschlüsselte Datenübertragung sichergestellt.

Die gesendeten Informationen werden dazu verwendet, die Schutzfunktionen unserer Dienste und Produkte zu verbessern.

6. Das Produkt auf dem aktuellen Stand halten

Automatische Updates

In F-Secure Mobile Security ist ein automatischer Update-Dienst integriert, der die Virendefinitionsdatenbank der Anwendung regelmäßig aktualisiert. Nur eine aktuelle Virendefinitionsdatenbank schützt Ihr Gerät vor den neuesten Viren. Automatische Updates werden durchgeführt, sobald Sie Ihr Produkt aktiviert haben.

Die Anwendung benötigt für die Updates eine aktive Internetverbindung. Wenn eine Verbindung mit dem Internet verfügbar ist, prüft die Anwendung, wann die Virendefinitionsdatenbank zuletzt aktualisiert wurde, und lädt nötigenfalls neue Updates herunter.

Manuelle Updates

So aktualisieren Sie die Anwendung manuell:

1. Navigieren Sie zu **Virenschutz** und drücken Sie die Auswahl Taste.
2. Wählen Sie **Jetzt aktualisieren** aus.
3. Wählen Sie den Internet-Zugriffspunkt für die Verbindung mit dem Update-Server. Die aktualisierte Virendefinitionsdatenbank wird von der Anwendung heruntergeladen und sofort eingesetzt.
4. Drücken Sie nach Abschluss des Updates auf **Ja**, um Ihr Gerät nach Viren zu durchsuchen, wenn Sie dazu aufgefordert werden. Weitere Informationen hierzu finden Sie im Abschnitt "**Scannen nach Viren**" weiter oben.

Versions- Updates

Wenn eine neue F-Secure Mobile Security-Version verfügbar ist, fordert Sie eine Meldung zum Herunterladen auf. Die Anwendung startet automatisch neu, wenn das Update abgeschlossen ist.

Technischer Support

Die Hauptansicht der Benutzeroberfläche zeigt die Sicherheitsübersicht und den aktuellen Status an.

Wenn Ihr Gerät laut Statusanzeige nicht geschützt ist, befolgen Sie diese Anweisungen:

1. Navigieren Sie zu **Sicherheitsübersicht** und drücken Sie die Auswahl Taste.
2. Wählen Sie das Element mit einem roten oder gelben Statussymbol aus und drücken Sie die Auswahl Taste, um das Problem zu beheben.

Für weitere Informationen laden Sie den *F-Secure Mobile Security for S60 User's Guide* (nur auf Englisch verfügbar) unter <http://mobile.f-secure.com/> herunter.

Wenn Sie Fragen zur Anwendung haben, die nicht im Handbuch oder in den Online-Diensten beantwortet werden, können Sie sich an Ihren lokalen F-Secure-Händler oder direkt an die F-Secure Corporation wenden.

HAFTUNGSAUSSCHLUSS

"F-Secure" und das Dreieckssymbol sind eingetragene Marken der F-Secure Corporation, ebenso sind F-Secure-Produktnamen und -Symbole/-Logos entweder Marken oder eingetragene Marken der F-Secure Corporation. Alle in diesem Handbuch erwähnten Produktnamen sind Marken der jeweiligen Unternehmen. Die F-Secure Corporation verzichtet auf Eigentumsansprüche bezüglich Marken und Namen von Dritten. Die F-Secure Corporation ist bei der Bereitstellung aller Informationen um äußerste Genauigkeit bemüht. Es wird jedoch keine Haftung für Fehler oder Auslassungen übernommen. Die F-Secure Corporation behält sich das Recht vor, in diesem Handbuch angegebene technische Daten ohne Vorankündigung zu ändern.

Sofern nicht anders angegeben, sind die in Beispielen verwendeten Unternehmen, Namen und Angaben frei erfunden. Ohne ausdrückliche schriftliche Genehmigung der F-Secure Corporation darf dieses Dokument weder vollständig, noch in Teilen, und in keiner erdenklichen Form, weder elektronisch noch mechanisch, zu keinem erdenklichen Zweck vervielfältigt oder übertragen werden.

Dieses Produkt unterliegt eventuell einem oder mehreren F-Secure-Patenten, einschließlich der folgenden:

GB2353372, GB2366691, GB2366692, GB2366693, GB2367933, GB2368233, GB2374260

Copyright © 2009 F-Secure Corporation. Alle Rechte vorbehalten.

