

# F-Secure Mobile Security™ for S60

## 1. Instalace a aktivace

**Předchozí verze** Předchozí verzi aplikace F-Secure Mobile Security není třeba odinstalovat. Po instalaci nové verze zkontrolujte nastavení aplikace F-Secure Mobile Security.

**Instalace** **Způsoby instalace:**

- Stáhněte instalační soubor do počítače a přesuňte ho do zařízení.
- Stáhněte instalační soubor do počítače a nainstalujte produkt pomocí softwaru Nokia PC Suite.
- Stáhněte instalaci přímo do zařízení. Instalace se spustí automaticky.

Pokud vás o to instalace požádá, zařízení po instalaci restartujte. Je-li instalace připravena, je třeba produkt aktivovat. Pokud produkt neaktivujete, nechrání vaše zařízení.

**Aktivace** **Spuštění aktivace:**

1. Otevřete aplikaci. Zobrazí se uvítací obrazovka.
2. Stiskněte klávesu **Pokračovat**.
3. Vyberte typ aktivace:
  - Chcete-li zahájit zkušební období, vyberte pro typ aktivace možnost **Bezplatná zkušební verze** (je-li dostupná) a stiskněte klávesu **Pokračovat**.
  - Chcete-li používat verzi s plnou licencí, vyberte pro typ aktivace možnost **Registrační číslo** a stiskněte klávesu **Pokračovat**. Zadejte registrační číslo a stiskněte klávesu **OK**.
4. Stiskněte klávesu **Ano** a vyberte přístupový bod k Internetu, kterým se připojíte k aktualizací službě, a začněte stahovat aktualizace.  
Aplikace se připojí k aktualizací službě a odešle vaše registrační číslo. Během první aktualizace aplikace stáhne nejnovější databázi definic virů.
5. Po dokončení stahování bude zobrazena zpráva s informací, že registrace byla úspěšná a že aplikace je aktivována. Aktivaci dokončíte stisknutím klávesy **OK**.
6. Po dokončení aktivace zkontrolujte zařízení na výskyt virů, abyste se ujistili, že je zařízení čisté. Další informace naleznete v následující části **Kontrola výskytu virů**.



*Kdykoli vás o to aplikace požádá, měli byste zařízení zkontrolovat.*

## 2. Kontrola výskytu virů

F-Secure Mobile Security operuje na pozadí a automaticky kontroluje soubory.

1. Pokud je při kontrole v reálném čase nalezen virus, zobrazí se zpráva. Chcete-li zobrazit infikované soubory, stiskněte klávesu **Ano**. Chcete-li toto dialogové okno zavřít, stiskněte klávesu **Ne**.
2. Zobrazení Infekce obsahuje seznam infikovaných souborů v zařízení a stav těchto souborů (v karanténě nebo uvolněno).

Zobrazení dalších podrobností o infikovaném souboru:

1. Přejděte k infikovanému souboru a stiskněte klávesu pro výběr.
2. Vyberte možnost **Zobrazit**.
3. Podrobnosti infekce zobrazují cestu a název souboru infikovaného souboru a název viru, který tento soubor infikoval.

### Zpracování infikovaných souborů

**Způsoby zpracování infikovaných souborů:**

1. Přejděte v zobrazení infekcí k infikovanému souboru, který chcete zpracovat.
2. Stiskněte klávesu pro výběr.
3. Vyberte jednu z následujících akcí:
  - **Odstranit** – odstraní infikovaný soubor. Jedná se o doporučenou možnost. Soubor bude ze zařízení zcela odstraněn.
  - **Karanténa** – pokud infikovaný soubor ještě není v karanténě, umístí ho do karantény. Soubor umístěný do karantény je uzamknut a pokud je aplikace F-Secure Mobile Security spuštěna, nemůže soubor zařízení poškodit.
  - **Uvolnit** – uvolní soubor z karantény. Uvolněný soubor již dále nebude uzamknutý. Přístup k tomuto souboru je na vaše riziko.

## 3. Ochrana proti neoprávněnému síťovému provozu

Brána firewall operuje v aplikaci F-Secure Mobile Security bezobslužně na pozadí. Monitoruje příchozí a odchozí síťový a internetový provoz a chrání uživatele před pokusy o vniknutí. Předem nadefinované úrovně brány firewall umožňují uživateli změnit úroveň ochrany podle vlastních potřeb.


### Výběr úrovně zabezpečení

**Výběr úrovně zabezpečení:**

1. Přejděte k položce **Nastavení** a stiskněte klávesu pro výběr.
2. Ze seznamu nastavení vyberte možnost **Brána firewall**.
3. Vyberte požadovanou úroveň brány firewall:
  - **Zakázat vše** – zastavuje veškerý síťový provoz.
  - **Vysoká** – povoluje většinu běžně používaných aplikací a blokuje veškerý příchozí provoz.
  - **Normální** – povoluje všechna odchozí připojení a blokuje veškerý příchozí provoz.
  - **Povolit vše** – povoluje veškerý síťový provoz.
  - **Vlastní** – povoluje síťový provoz na základě vlastních pravidel uživatele. Chcete-li upravit sadu vlastních pravidel, vyberte úroveň zabezpečení **Vlastní** a položky **Možnosti > Upravit vlastní pravidla**.

## 4. Ochrana důvěrných informací

Pomocí ochrany proti krádežím zajistíte, že vaše zařízení a data na něm uložená nebudou v případě krádeže zařízení zneužita.


-  *Vzhledem k tomu, že paměťové karty lze snadno vyjmout, doporučujeme ukládat důvěrné informace do paměti zařízení, kterou lze pomocí ochrany proti krádežím zamknout nebo vymazat.*

### Použití zamknutí zařízení

Ochrana proti krádežím dokáže zařízení automaticky zamknout, dojde-li v zařízení ke změně karty SIM. Zamknuté zařízení lze odemknout pouze pomocí kódu zamknutí.

#### Nastavení kódu zamknutí:

- Přejděte k položce **Nastavení** a stiskněte klávesu pro výběr.
- Ze seznamu nastavení vyberte možnost **Ochrana proti krádežím**.
- Zadejte **Kód zamknutí**. Kód zamknutí musí mít nejméně 5 znaků. Kód uchovávejte na bezpečném místě.

-  *Nastavení ochrany proti krádežím je chráněno vaším kódem zamknutí. Abyste mohli změnit kterákoli nastavení ochrany proti krádežím, je třeba zadat aktuální kód zamknutí.*

- Chcete-li zařízení zamknout při změně karty SIM, vyberte možnost **Ano** u položky **Zamknout při změně karty SIM**.

### Používání vzdálené ochrany proti krádežím

Vzdálená ochrana proti krádežím umožňuje odeslat do zařízení textovou zprávu SMS, která bude obsahovat kód zamknutí, a tím zařízení zamknout, nebo kód vymazání, a tím vymazat všechny informace v zařízení.

#### Nastavení vzdáleného zamknutí:

- Přejděte k položce **Nastavení** a stiskněte klávesu pro výběr.
- Ze seznamu nastavení vyberte možnost **Ochrana proti krádežím**.
- Chcete-li umožnit vzdálené zamknutí zařízení, postupujte podle těchto pokynů:
  - Pokud jste ho ještě nevytvořili, zadejte **kód zamknutí**.
  - Zapněte funkci **Vzdálené zamknutí**.Zamknuté zařízení lze odemknout pouze pomocí kódu zamknutí.
- Chcete-li umožnit vzdálené vymazání zařízení, postupujte podle těchto pokynů:
  - Zadejte **Kód vymazání**. Kód vymazání musí mít nejméně 8 znaků. Kód uchovávejte na bezpečném místě.
  - Zapněte funkci **Vzdálené vymazání**.

Vymazání odstraní ze zařízení veškerá data, která jsou na něm uložena.

#### Vzdálené zamknutí nebo vymazání zařízení:

- Chcete-li zařízení zamknout, pošlete do zařízení SMS s následující zprávou:  
#LOCK#<kód zamknutí> (Například: #LOCK#abcd1234)
- Chcete-li zařízení vymazat, pošlete do zařízení SMS s následující zprávou:  
#WIPE#<kód vymazání> (Například: #WIPE#abcd1234)

## 5. Zajištění aktuálnosti produktu

|                                |   |
|--------------------------------|---|
| <b>Automatické aktualizace</b> | <p>Součástí aplikace F-Secure Mobile Security je služba zajišťující automatické aktualizace; to znamená, že databáze definic virů v aplikaci je pravidelně aktualizována. Pouze aktuální databáze definic virů totiž dokáže zařízení chránit proti nejnovějším virům. Automatické aktualizace jsou spuštěny po aktivaci produktu.</p> <p>Aby mohla být aplikace aktualizována, vyžaduje aktivní připojení k Internetu. Když je k dispozici připojení k Internetu, aplikace zkontroluje čas poslední aktualizace databáze definic virů a v případě potřeby stáhne nové aktualizace.</p>                          |
| <b>Ruční aktualizace</b>       | <p><b>Ruční aktualizace aplikace:</b></p> <ol style="list-style-type: none"><li>1. Přejděte k položce <b>Ochrana proti virům</b> a stiskněte klávesu pro výběr.</li><li>2. Vyberte možnost <b>Aktualizovat nyní</b>.</li><li>3. Vyberte přístupový bod k Internetu pro připojení k aktualizacímu serveru. Aplikace stáhne nejnovější databázi definic virů a ihned ji začne používat.</li><li>4. Pokud budete po dokončení aktualizace vyzváni, abyste zařízení zkontrolovali na výskyt virů, stiskněte klávesu <b>Ano</b>. Další informace naleznete v předchozí části <b>Kontrola výskytu virů</b>.</li></ol> |
| <b>Aktualizace verzí</b>       | <p>Je-li k dispozici nová verze aplikace F-Secure Mobile Security, objeví se zpráva, která vás požádá o stažení této aktualizace. Po dokončení aktualizace se aplikace automaticky restartuje.</p>  |

## Technická podpora

Máte-li zájem o další informace, stáhněte si z adresy <http://mobile.f-secure.com/> příručku *F-Secure Mobile Security for S60 User's Guide* (v angličtině).

Máte-li ohledně aplikace jakékoli otázky, na které jste nenašli odpověď v průvodcích ani ve službách online, můžete kontaktovat svého místního prodejce F-Secure nebo přímo společnost F-Secure Corporation.

---

### PRÁVNÍ OMEZENÍ

F-Secure a trojúhelníkové logo jsou registrované ochranné známky společnosti F-Secure Corporation a názvy, symboly a loga produktů F-Secure jsou ochranné známky nebo registrované ochranné známky společnosti F-Secure Corporation. Všechny názvy produktů uvedené v této příručce jsou ochranné známky nebo registrované ochranné známky příslušných společností. Společnost F-Secure Corporation se zříká vlastnických zájmů týkajících se značek a názvů jiných vlastníků. Přestože společnost F-Secure Corporation vynakládá maximální úsilí na zajištění přesnosti těchto informací, není zodpovědná za chyby a nepřesnosti, které se zde mohou vyskytnout. Společnost F-Secure Corporation si vyhrazuje právo měnit specifikace uvedené v tomto dokumentu bez předchozího upozornění.

Není-li uvedeno jinak, jsou společnosti, názvy a data, jež jsou použita v příkladech, smyšlená. Žádná z částí tohoto dokumentu nesmí být reprodukována nebo přenášena v jakémkoliv formě nebo jakýmkoliv prostředky, elektronickými či mechanickými, za jakýmkoliv účelem, bez explicitního písemného povolení od společnosti F-Secure Corporation.

Tento produkt může být chráněn některými z následujících patentů společnosti F-Secure:

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

Copyright © 2009 F-Secure Corporation Všechna práva vyhrazena.

