

# F-Secure Mobile Security™ for S60

## 1. Instalace a aktivace

**Předchozí verze** Předchozí verzi aplikace F-Secure Mobile Anti-Virus 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 tlačítko **Pokračovat**.
3. Vyberte typ aktivace:
  - Chcete-li produkt aktivovat pouze s funkcí Ochrana proti krádežím, vyberte typ aktivace **Pouze ochrana proti krádežím** a stiskněte tlačítko **Pokračovat**.
  - Chcete-li používat verzi s plnou licencí, vyberte pro typ aktivace možnost **Registrační číslo** a stiskněte tlačítko **Pokračovat**. Zadejte registrační číslo a stiskněte tlačítko **OK**.
4. Stiskněte tlačítko **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. Jakmile produkt stáhne všechny potřebné aktualizace, aplikace je úplná. Stisknutím tlačítka **Pokračovat** aktivaci ukončete.

Po dokončení aktivace zkontrolujte zařízení na výskyt virů, abyste se ujistili, že je zařízení čisté. Další informace naleznete v následující části **Kontrola výskytu virů**.



*Přítomnost virů v zařízení byste měli kontrolovat pokaždé, když o to aplikace požádá.*

## 2. Kontrola výskytu virů

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

1. Najde-li aplikace F-Secure Mobile Security při kontrole v reálném čase vir, upozorní vás na to. Po stisknutí tlačítka **Ano** si můžete ihned prohlédnout infikované soubory. Pokud je chcete zobrazit později, stiskněte tlačítko **Ne**.
2. Zobrazení Infekce obsahuje seznam infikovaných souborů v zařízení a informuje, zda je soubor momentálně v karanténě, nebo je uvolněný.

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, název infikovaného souboru a název viru, který tento soubor infikoval.

### Zpracování infikovaných souborů

#### Zpracování infikovaných souborů:

1. Ve zobrazení Infekce přejděte 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 soubor do karantény. Soubor umístěný do karantény je uzamčen 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. Zabránění neoprávněnému síťovému přenosu

Brána firewall pracuje v aplikaci F-Secure Mobile Security bezobslužně na pozadí. Monitoruje příchozí a odchozí síťový a internetový provoz a chrání uživatele před pokusy o vniknutí. Předdefinované úrovně brány firewall umožňují podle potřeby změnit úroveň ochrany.


### 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:
  - **Odmítnout vše** – Zastavuje veškerý síťový přenos.
  - **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 přenos.
  - **Vlastní** – Povoluje síťový přenos na základě pravidel uživatele. Chcete-li upravit sadu vlastních pravidel, vyberte úroveň zabezpečení **Vlastní** a položky **Možnosti > Upravit vlastní pravidla**.

## 4. Ochrana důvěrných informací

Anti-Theft pomáhá zajistit, aby vaše zařízení a uložená data nebyla v případě krádeže zařízení zneužita.


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

### Použití zámku zařízení

Anti-Theft dokáže zařízení automaticky zamknout, dojde-li v zařízení ke změně karty SIM. Zamknuté zařízení lze odemknout jen pomocí kódu zamknutí.

#### Nastavení kódu zamknutí:

1. Přejděte k položce **Nastavení** a stiskněte klávesu pro výběr.
2. Ze seznamu nastavení vyberte možnost **Anti-Theft**.
3. Zadejte **Kód zamknutí**. Kód zamknutí musí mít nejméně 5 znaků. Kód uchovávejte na bezpečném místě.

-  *Nastavení Anti-Theft je chráněno vaším kódem zamknutí. Aby bylo možné změnit nastavení Anti-Theft, je nutné zadat aktuální kód zamknutí.*

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

### Použití vzdálené ochrany proti krádežím

Vzdálená ochrana proti krádežím umožňuje odeslat do zařízení textovou zprávu SMS s kódem zamknutí. To umožňuje zařízení lokalizovat nebo zamknout. Můžete také odeslat kód vymazání, a smazat tak všechny informace v zařízení.


#### Nastavení vzdáleného zamknutí:

1. Přejděte k položce **Nastavení** a stiskněte klávesu pro výběr.
2. Ze seznamu nastavení vyberte možnost **Anti-Theft**.
3. Chcete-li aktivovat vzdálené zamknutí zařízení, postupujte podle těchto pokynů:
  - a. Pokud jste ho ještě nevytvořili, zadejte **kód zamknutí**.
  - b. Zapněte funkci **Vzdálené zamknutí**.Zamknuté zařízení lze odemknout jen pomocí kódu zamknutí.
4. Chcete-li umožnit vzdálené vymazání zařízení, postupujte podle těchto pokynů:
  - a. Zadejte **kód vymazání**. Kód vymazání musí mít nejméně 8 znaků. Kód uchovávejte na bezpečném místě.
  - b. Zapněte funkci **Vzdálené vymazání**.Vymazání odstraní ze zařízení veškerá data, která jsou v něm uložena.

#### Vzdálené zamknutí nebo vymazání zařízení:

Svému zařízení odešlete následující textovou zprávu SMS.


- Chcete-li zařízení zamknout, odešlete:  
#LOCK#<kód zamknutí> (např. #LOCK#abcd1234)
- Chcete-li zařízení vymazat, odešlete:  
#WIPE#<kód vymazání> (např. #WIPE#abcd1234)
- Chcete-li zařízení lokalizovat, odešlete:  
#LOCATE#<kód zamknutí> (např. #LOCATE#abcd1234)

-  *Anti-Theft neukládá údaje o umístění. Jediné informace týkající se umístění jsou obsaženy v textové zprávě SMS, která vám byla zaslána.*

## 5. Ochrana při procházení webu

Ochrana procházení poskytuje ochranu před weby, které mohou odcizit vaše osobní údaje, jako jsou čísla platebních karet, informace o účtu uživatele a hesla.

Tato funkce kontroluje weby, které procházíte pomocí výchozího prohlížeče vašeho zařízení. Jestliže použijete prohlížeč jiného výrobce, nebude ochrana procházení webu fungovat.

 *Než začnete funkci Ochrana procházení používat, vypněte webový prohlížeč a vymažte jeho mezipaměť.*

### Zapnutí funkce Ochrana procházení:


1. Přejděte k položce **Nastavení** a stiskněte klávesu pro výběr.
2. Ze seznamu nastavení vyberte možnost **Ochrana procházení**.
3. Zapněte funkci **Ochrana procházení**.
4. V části **Používaná síť** vyberte, zda chcete funkci Ochrana procházení používat neustále, nebo jen když procházíte web prostřednictvím sítě svého operátora:
  - Chcete-li používat funkci Ochrana procházení, jen když používáte síť svého operátora, vyberte možnost **Pouze můj operátor**.
  - Chcete-li ponechat ochranu zapnutou, když cestujete nebo se pohybujete mimo síť svého operátora, vyberte možnost **Všichni operátoři**.

### Výpis ochrany osobních údajů

Kvůli zachování kvality služby může funkce Ochrana procházení automaticky odesílat k analýze informace o webech, které obsahují škodlivý obsah. Můžete vybrat, jaké informace budou k analýze odesílány.

### Změna režimu ochrany osobních údajů:

1. Přejděte k položce **Nastavení** a stiskněte klávesu pro výběr.
2. Ze seznamu nastavení vyberte možnost **Jiná nastavení**.
3. V režimu ochrany osobních údajů postupujte následovně.
  - Chcete-li odesílat pouze statistiku ochrany procházení a informace o připojení k serveru, vyberte možnost **Pouze statistika**.
  - Chcete-li odesílat statistiku a informace o webech, které nebyly analyzovány nebo obsahovaly škodlivý obsah, vyberte možnost **Povolit vše**.

 *Doporučujeme ponechat režim ochrany osobních údajů nastavený na hodnotu **Povolit vše**, čímž je dosaženo nejlepší kvality služby.*

### Výpis ochrany osobních údajů

Odesláním informací není ohroženo vaše soukromí.

Ačkoli odeslané informace mohou být v některých jurisdikcích považovány za osobní, vaše soukromí je během tohoto procesu chráněno. Informace jsou přenášeny bezpečně; jsou z nich odebrány všechny nadbytečné osobní údaje a zpracovávají se anonymně v souhrnném formátu. Tím je zajištěno, aby tyto informace nemohly být s vámi žádným způsobem spojovány. Odeslané informace neobsahují údaje o uživatelském účtu, adrese IP ani informace o licenci. Kvůli větší ochraně soukromí je při přenosu informací použito šifrování.

Odeslané informace slouží ke zlepšení ochranných funkcí našich produktů a služeb.

## 6. Zajištění aktuálnosti produktu

**Automatické aktualizace** 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.

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.

**Ruční verze** **Ruční aktualizace aplikace:**

1. Přejděte k položce **Ochrana proti virům** a stiskněte klávesu pro výběr.
2. Vyberte možnost **Aktualizovat nyní**.
3. Vyberte přístupový bod k Internetu pro připojení k aktualizacímu serveru. Aplikace stáhne nejnovější databázi definic virů a ihned ji začne používat.
4. Pokud budete po dokončení aktualizace vyzváni, abyste zařízení zkontrolovali na výskyt virů, stiskněte klávesu **Ano**. Další informace naleznete v předchozí části **Kontrola výskytu virů**.

**Aktualizace verze** 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.

## Technická podpora

Hlavní zobrazení uživatelského rozhraní poskytuje přehled o zabezpečení a aktuálním stavu.

Jestliže stav indikuje, že zařízení není chráněno, postupujte podle těchto pokynů:

1. Přejděte k položce **Přehled zabezpečení** a stiskněte klávesu pro výběr.
2. Vyberte položku označenou buď červenou, nebo žlutou ikonou stavu a stisknutím klávesy pro výběr problém vyřešte.

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 zřiká 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.

