

F-Secure Mobile Security™ for S60

1. Instalowanie i aktywowanie

Poprzednia wersja Odinstalowanie poprzedniej wersji programu F-Secure Mobile Anti-Virus nie jest konieczne. Po zainstalowaniu nowej wersji należy sprawdzić ustawienia programu F-Secure Mobile Security.

Instalowanie **Aby przeprowadzić instalację:**

- Pobierz plik instalacyjny na komputer, a następnie przenieś ten plik na urządzenie.
- Pobierz plik instalacyjny na komputer i zainstaluj produkt przy użyciu oprogramowania Nokia PC Suite.
- Można też pobrać plik instalacyjny bezpośrednio na urządzenie. Instalacja rozpocznie się automatycznie.

Po zakończeniu instalacji uruchom ponownie urządzenie (jeśli instalator wyświetli odpowiedni monit). Po zainstalowaniu produktu należy go aktywować. Produkt nie chroni urządzenia, jeśli nie jest aktywowany.

Aktywowanie **Aby rozpocząć aktywację, wykonaj następujące czynności:**

1. Otwórz aplikację. Zostanie wyświetlony ekran powitalny.
2. Naciśnij przycisk **Kontynuuj**.
3. Wybierz typ aktywacji:
 - Aby aktywować produkt tylko z aktywną funkcją zabezpieczenia na wypadek kradzieży, wybierz opcję **Tylko zabezpieczenie przed kradzieżą** jako typ aktywacji i naciśnij przycisk **Kontynuuj**.
 - Aby używać w pełni licencjonowanej wersji, wybierz jako typ aktywacji opcję **Numer subskrypcji**, a następnie naciśnij przycisk **Kontynuuj**. Wprowadź numer subskrypcji i naciśnij przycisk **OK**.
4. Naciśnij przycisk **Tak**, a następnie wybierz punkt dostępu do Internetu, aby połączyć się z usługą aktualizacji i rozpocząć pobieranie aktualizacji. Aplikacja nawiąże połączenie z usługą aktualizacji i prześle podany numer subskrypcji. Podczas pierwszej aktualizacji aplikacja pobiera najnowszą bazę danych definicji wirusów.
5. Po pobraniu przez produkt wszystkich koniecznych aktualizacji aplikacja będzie kompletna. Naciśnij przycisk **Kontynuuj**, aby zakończyć aktywację.

Po zakończeniu aktywacji należy przeskanować urządzenie w poszukiwaniu wirusów, aby sprawdzić, czy nie zostało zainfekowane. Odpowiednie instrukcje można znaleźć w sekcji **Skanowanie w poszukiwaniu wirusów** poniżej.



Po wyświetleniu przez aplikację odpowiedniego monitu należy przeskanować urządzenie.

2. Skanowanie w poszukiwaniu wirusów

Aplikacja F-Secure Mobile Security pracuje w tle i skanuje pliki automatycznie.

1. Produkt F-Secure Mobile Security wyświetla powiadomienie w przypadku wykrycia wirusa podczas skanowania w czasie rzeczywistym. Naciśnij przycisk **Tak**, aby od razu przejrzeć zainfekowane pliki, lub przycisk **Nie**, aby przejrzeć je później.
2. Widok infekcji zawiera listę zainfekowanych plików w pamięci urządzenia i stan każdego pliku (poddany kwarantannie lub zwolniony).

Aby wyświetlić szczegółowe informacje o zainfekowanym pliku, wykonaj następujące czynności:

1. Przewiń listę do zainfekowanego pliku i naciśnij klawisz wyboru.
2. Wybierz opcję **Wyświetl**.
3. W widoku szczegółów infekcji zostaną wyświetlone informacje o ścieżce i nazwie zainfekowanego pliku oraz nazwie wirusa, który zainfekował ten plik.

Przetwarzanie zainfekowanych plików

Aby przetworzyć zainfekowane pliki, wykonaj następujące czynności:

1. W widoku infekcji wskaż zainfekowany plik do przetworzenia.
2. Naciśnij klawisz wyboru.
3. Wybierz jedną z następujących czynności:
 - **Usuń** — usunięcie zainfekowanego pliku. Jest to zalecana opcja. Plik zostanie całkowicie usunięty z urządzenia.
 - **Poddaj kwarantannie** — umieszczenie zainfekowanego pliku w kwarantannie, jeśli nie zostało to jeszcze zrobione. Gdy program F-Secure Mobile Security działa, plik poddany kwarantannie jest zablokowany i nie może wyrządzić szkód na urządzeniu.
 - **Zwolnij** — zwolnienie pliku z kwarantanny. Zwolnienie pliku powoduje jego odblokowanie. Użytkownik korzysta z takiego pliku na własne ryzyko.

3. Blokowanie nieautoryzowanego ruchu sieciowego

Zapora w programie F-Secure Mobile Security działa dyskretnie w tle. Zapora monitoruje przychodzący i wychodzący ruch sieciowy i internetowy, a także chroni przed próbami włamań. Wstępnie zdefiniowane poziomy zapory umożliwiają zmianę poziomu zabezpieczeń zgodnie z potrzebami.


Wybieranie poziomu zabezpieczeń

Aby wybrać poziom zabezpieczeń, wykonaj następujące czynności:

1. Wskaż opcję **Ustawienia** i naciśnij klawisz wyboru.
2. Z listy ustawień wybierz opcję **Zapora**.
3. Wybierz żądany poziom zapory:
 - **Zabroń wszystko** — blokowanie całego ruchu sieciowego.
 - **Wysoki** — zezwalanie na najczęściej używane aplikacje i blokowanie całego ruchu przychodzącego.
 - **Normalny** — zezwalanie na wszystkie połączenia wychodzące i blokowanie całego ruchu przychodzącego.
 - **Zezwalaj na wszystko** — zezwalanie na cały ruch sieciowy.
 - **Niestandardowy** — zezwalanie na ruch sieciowy na podstawie własnych reguł. Aby edytować zestaw reguł niestandardowych, wybierz opcję **Opcje > Edytuj reguły niestandardowe**, gdy włączony jest **Niestandardowy** poziom zabezpieczeń.

4. Ochrona poufnych informacji

Funkcja Anti-Theft pomaga chronić urządzenie i przechowywane na nim dane przed niewłaściwym użyciem w przypadku kradzieży urządzenia.


-  *Karty pamięci można łatwo wyjąć z urządzenia, dlatego ze względów bezpieczeństwa poufne informacje należy przechowywać w pamięci urządzenia, którą można zablokować lub wyczyścić przy użyciu funkcji Anti-Theft.*

Używanie blokady urządzenia

Anti-Theft można skonfigurować tak, aby urządzenie zostało zablokowane po zmianie karty SIM. W razie zablokowania urządzenia można je odblokować tylko przy użyciu kodu blokady.

Aby skonfigurować blokadę urządzenia, wykonaj następujące czynności:

1. Wskaż opcję **Ustawienia** i naciśnij klawisz wyboru.
2. Na liście ustawień wybierz opcję **Anti-Theft**.
3. Wprowadź **Kod blokady**. Kod blokady musi zawierać co najmniej 5 znaków. Przechowuj ten kod w bezpiecznym miejscu.

-  *Kod blokady chroni ustawienia funkcji Anti-Theft. Aby móc zmienić jakiegokolwiek ustawienia funkcji Anti-Theft, należy podać bieżący kod blokady.*

4. Jeśli urządzenie ma być blokowane po zmianie karty SIM, wybierz opcję **Tak** w ustawieniu **Zablokuj po zmianie karty SIM**.

Używanie zdalnego Anti-Theft

Zdalne Anti-Theft umożliwia zlokalizowanie urządzenia lub zablokowanie go przez wysłanie na urządzenie wiadomości SMS z kodem blokady albo wyczyszczenie wszystkich zawartych na urządzeniu informacji przez wysłanie wiadomości SMS z kodem czyszczenia.

Aby skonfigurować blokadę zdalną, wykonaj następujące czynności:

1. Wskaż opcję **Ustawienia** i naciśnij klawisz wyboru.
2. Na liście ustawień wybierz opcję **Anti-Theft**.
3. Jeśli chcesz uzyskać możliwość zdalnego blokowania urządzenia, postępuj zgodnie z poniższymi instrukcjami:
 - a. Wprowadź **Kod blokady**, jeśli nie został on już utworzony.
 - b. Włącz funkcję **Blokada zdalna**.

W razie zablokowania urządzenia można je odblokować tylko przy użyciu kodu blokady.


4. Jeśli chcesz uzyskać możliwość zdalnego czyszczenia urządzenia, postępuj zgodnie z poniższymi instrukcjami:
 - a. Wprowadź **Kod czyszczenia**. Kod czyszczenia musi zawierać co najmniej 8 znaków. Przechowuj ten kod w bezpiecznym miejscu.
 - b. Włącz funkcję **Zdalne czyszczenie**.

Wyczyszczenie urządzenia powoduje usunięcie wszystkich zapisanych na nim danych.

Aby zdalnie zablokować lub wyczyścić urządzenie, wykonaj następujące czynności:

Wyślij na urządzenie wiadomość SMS o następującej treści.

- Aby zablokować urządzenie, wyślij kod:
#LOCK#<kod blokady> (na przykład: #LOCK#abcd1234)
- Aby wyczyścić urządzenie, wyślij kod:
#WIPE#<kod czyszczenia> (na przykład: #WIPE#abcd1234)
- Aby zlokalizować urządzenie, wyślij kod:
#LOCATE#<kod lokalizacji> (na przykład: #LOCATE#abcd1234)

-  *Anti-Theft nie przechowuje jakiegokolwiek danych dotyczących lokalizacji. Informacje na temat lokalizacji znajdują się tylko w wysłanej wiadomości SMS.*

5. Ochrona podczas przeglądania sieci Web

Funkcja ochrony przeglądania chroni użytkownika przed witrynami, na których może dojść do kradzieży informacji osobistych, w tym numerów kart kredytowych, informacji o koncie oraz haseł.

Ochrona przeglądania polega na sprawdzeniu witryny sieci Web otwieranej za pomocą domyślnej przeglądarki na urządzeniu. Funkcja ochrony przeglądania nie zabezpiecza przed zagrożeniami w przypadku korzystania z innej przeglądarki.

 *Wyłącz przeglądarkę sieci Web i wyczyść jej pamięć podręczną przed rozpoczęciem korzystania z ochrony przeglądania.*

Aby włączyć funkcję ochrony przeglądania, należy wykonać następujące czynności:


1. Wskaż opcję **Ustawienia** i naciśnij klawisz wyboru.
2. Na liście ustawień wybierz opcję **Ochrona przeglądania**.
3. Włącz opcję **Ochrona przeglądania**.
4. W sekcji **Sieć do użycia** wybierz, czy ochrona przeglądania ma działać cały czas, czy tylko podczas przeglądania Internetu w sieci Twojego operatora.
 - Wybierz opcję **Tylko mój operator**, aby ochrona przeglądania działała tylko podczas korzystania z sieci Twojego operatora.
 - Wybierz ustawienie **Wszyscy operatorzy**, aby opcja przeglądania była włączona w podróży, gdy nie korzystasz z sieci swojego operatora.

Oświadczenie prywatności

Aby zachować jakość usługi, funkcja ochrony przeglądania może automatycznie wysyłać do analizy informacje o witrynach sieci Web, które zawierają szkodliwą zawartość. Można wybrać informacje, które mają być przesyłane do analizy.

Aby zmienić tryb prywatności, należy wykonać następujące czynności:

1. Wskaż opcję **Ustawienia** i naciśnij klawisz wyboru.
2. Na liście ustawień wybierz opcję **Inne ustawienia**.
3. Wybierz jedną z opcji dla trybu prywatności:
 - Wybierz opcję **Tylko statystyka**, aby wysyłać tylko informacje statystyczne dotyczące ochrony przeglądania wraz z informacjami na temat połączenia z serwerem.
 - Wybierz opcję **Zezwalaj na wszystko**, aby przysyłać informacje statystyczne wraz z informacjami o witrynach sieci Web, które nie zostały jeszcze przeanalizowane lub zawierają szkodliwą zawartość.

 *Aby zapewnić najlepszą jakość usługi, zalecane jest pozostawienie opcji **Zezwalaj na wszystko** dla trybu prywatności.*

Oświadczenie dotyczące prywatności

Przesyłanie informacji nie powoduje naruszenia prywatności użytkownika.

Przesyłane informacje mogą być uznawane za osobiste w niektórych prawodawstwach, jednak prywatność użytkownika jest chroniona w trakcie całego procesu. Informacje są bezpiecznie przesyłane po usunięciu wszystkich niepotrzebnych danych osobowych, a następnie anonimowo przetwarzane w zbiorczym formacie. Dzięki temu połączenie informacji z użytkownikiem jest niemożliwe. W przesyłanych informacjach nie są uwzględniane żadne dane dotyczące konta, adresu IP ani licencji. Dodatkowo prywatność użytkowników jest chroniona przy użyciu szyfrowania przesyłanych informacji.

Przesłane informacje są używane w celu ulepszania funkcji ochrony w usługach i produktach firmy F-Secure.

6. Aktualizowanie produktu

Aktualizacje automatyczne

Aplikacja F-Secure Mobile Security zawiera usługę automatycznej aktualizacji, co oznacza, że jej baza danych definicji wirusów jest regularnie aktualizowana. Tylko aktualna baza danych definicji wirusów zapewnia ochronę urządzenia przed najnowszymi wirusami. Aktualizacje automatyczne są przeprowadzane po uaktywnieniu produktu.

Do przeprowadzania aktualizacji niezbędne jest aktywne połączenie internetowe. Gdy jest dostępne połączenie z Internetem, aplikacja sprawdza termin ostatniej aktualizacji bazy danych definicji wirusów i w razie potrzeby pobiera nowe aktualizacje.

Ręczne wersji

Aby ręcznie zaktualizować aplikację, wykonaj następujące czynności:

1. Wskaż opcję **Ochrona przed wirusami** i naciśnij klawisz wyboru.
2. Wybierz opcję **Aktualizuj teraz**.
3. Wybierz punkt dostępu do Internetu, aby połączyć się z serwerem aktualizacji. Aplikacja pobierze najnowszą bazę danych definicji wirusów i natychmiast zacznie z niej korzystać.
4. Jeśli po zakończeniu aktualizacji zostanie wyświetlony monit o przeprowadzenie skanowania, naciśnij przycisk **Tak**, aby przeskanować urządzenie w poszukiwaniu wirusów. Odpowiednie instrukcje znajdują się w sekcji **Skanowanie w poszukiwaniu wirusów** powyżej.

Aktualizacje wersji

Gdy jest dostępna nowa wersja aplikacji F-Secure Mobile Security, pojawia się komunikat z pytaniem, czy ma ona zostać pobrana. Po zakończeniu aktualizacji aplikacja zostanie automatycznie uruchomiona ponownie.

Pomoc techniczna

W głównym widoku interfejsu użytkownika są wyświetlane informacje ogólne dotyczące zabezpieczeń wraz z bieżącym stanem produktu.

Jeśli informacje o stanie produktu wskazują, że urządzenie nie jest chronione, postępuj zgodnie z poniższymi instrukcjami:

1. Wskaż opcję **Przegląd zabezpieczeń** i naciśnij klawisz wyboru.
2. Wybierz element z czerwoną lub żółtą ikoną stanu i naciśnij klawisz wyboru, aby rozwiązać ten problem.

Więcej informacji można znaleźć w podręczniku *F-Secure Mobile Security for S60 User's Guide* (tylko w języku angielskim) dostępnym do pobrania z witryny <http://mobile.f-secure.com/>.

W razie pytań dotyczących aplikacji, na które nie udzielono odpowiedzi w podręcznikach ani w usługach online, można skontaktować się z lokalnym dystrybutorem produktów firmy F-Secure bądź bezpośrednio z firmą F-Secure Corporation.

ZRZECZENIE SIĘ ODPOWIEDZIALNOŚCI

„F-Secure” i symbol trójkąta są zastrzeżonymi znakami towarowymi firmy F-Secure Corporation, a nazwy produktów i symbole/logo firmy F-Secure są znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy F-Secure Corporation. Wszystkie nazwy produktów wymienione w niniejszej publikacji są znakami towarowymi lub zastrzeżonymi znakami towarowymi odpowiednich firm. Firma F-Secure Corporation nie rości sobie żadnych praw własności do znaków i nazw należących do innych firm. Mimo że firma F-Secure Corporation dołożyła wszelkich starań, aby niniejsze informacje były dokładne, to nie ponosi odpowiedzialności za jakiegokolwiek błąd i pominięcia występujące w tym tekście. Firma F-Secure Corporation zastrzega sobie prawo do modyfikowania parametrów technicznych przedstawionych w niniejszym dokumencie bez wcześniejszego powiadomienia.

Nazwy firm, osób i dane użyte jako przykłady w niniejszym tekście są fikcyjne, chyba że zaznaczono inaczej. Żaden fragment tego dokumentu nie może być kopiowany lub przekazywany w jakiegokolwiek formie ani za pomocą jakiegokolwiek urządzeń (elektronicznych czy mechanicznych), w jakimkolwiek celu, bez wyraźnej pisemnej zgody firmy F-Secure Corporation.

Ten produkt może być objęty patentem lub patentami firmy F-Secure, w tym następującymi:
GB2353372, GB2366691, GB2366692, GB2366693, GB2367933, GB2368233, GB2374260

Copyright © 2009 F-Secure Corporation. Wszelkie prawa zastrzeżone.

