

# F-Secure Mobile Security™ for Windows Mobile

## 1. Instalowanie i aktywowanie

### Poprzednia wersja

Jeśli na urządzeniu jest zainstalowana wcześniejsza wersja aplikacji F-Secure Mobile Security, należy ją zamknąć. Wcześniejsza wersja zostanie automatycznie usunięta podczas instalacji.

### Instalowanie

**Aby przeprowadzić instalację:**

1. Przenieś plik instalacyjny .cab do urządzenia.
2. Znajdź i wybierz plik .cab w Eksploratorze plików na urządzeniu.
3. Po wyświetleniu zapytania wybierz opcję **Tak**, aby przeprowadzić instalację.
4. Wybierz opcję **Tak**, aby wyrazić zgodę na warunki licencji.
5. Po zainstalowaniu aplikacji zostanie wyświetlony monit o ponowne uruchomienie urządzenia. Select **Tak**.
6. Po zainstalowaniu produktu należy go aktywować. Produkt nie chroni urządzenia, jeśli nie jest aktywowany.

### Aktywowanie


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


1. Select Po zainstalowaniu produktu F-Secure Mobile Security włącz urządzenie. Zostanie wyświetlone powiadomienie dotyczące aktywacji. Wybierz w nim opcję **Tak**.
2. Wybierz typ aktywacji:
  - Aby rozpocząć okres testowania, wybierz jako typ aktywacji opcję **Bezpłatne testowanie**, a następnie wybierz przycisk **Dalej**, LUB
  - Aby używać w pełni licencjonowanej wersji, wybierz jako typ aktywacji opcję **Numer subskrypcji**, a następnie wybierz przycisk **Dalej**. Wprowadź numer subskrypcji i wybierz przycisk **Dalej**.
3. Wybierz przycisk **Tak**, aby połączyć się z usługą aktualizacji. Aplikacja nawiąże połączenie z usługą aktualizacji i prześle podany numer subskrypcji. Podczas pierwszej aktualizacji aplikacja pobiera najnowszą bazę danych definicji wirusów.
4. Po ukończeniu pobierania zostanie wyświetlony komunikat, że rejestracja przebiegła pomyślnie i aplikacja jest aktywna. Wybierz przycisk **OK**, aby zakończyć aktywację.
5. Po zakończeniu aktywacji należy przeskanować urządzenie w poszukiwaniu wirusów w celu upewnienia się, że urządzenie jest oczyszczone. Więcej informacji można znaleźć w części „[Skanowanie w poszukiwaniu wirusów](#)”.

W przypadku używania bezpłatnej wersji próbnej aplikacji i posiadania ważnego kodu subskrypcji należy otworzyć menu *Kup* i wprowadzić kod subskrypcji, aby przeprowadzić aktywację.

## Uruchamianie produktu

Po przeprowadzeniu aktywacji program F-Secure Mobile Security będzie uruchamiany automatycznie po każdym włączeniu urządzenia.

1. W systemie Windows Mobile w wersji Professional lub Classic wybierz kolejno pozycje **Start→ Programy→  Mobile Security**.

W systemie Windows Mobile Standard wybierz pozycje **Start→  Mobile Security**.

2. Wybierz opcję **Tak**, jeśli zostanie wyświetlony monit o rozpoczęcie skanowania w poszukiwaniu wirusów.

## 2. Skanowanie w poszukiwaniu wirusów

Program F-Secure Mobile Security działa w tle i skanuje pliki automatycznie, gdy włączona jest funkcja skanowania w czasie rzeczywistym.

1. Jeśli podczas skanowania w czasie rzeczywistym zostanie wykryty wirus, pojawi się odpowiedni komunikat. Wybierz przycisk **Tak**, aby przejrzeć zainfekowane pliki, lub przycisk **Nie**, aby zamknąć widok.
2. Widok *Infekcje* zawiera listę zainfekowanych plików znalezionych na urządzeniu. Dla każdej pozycji na liście jest wyświetlany stan (Poddane kwarantannie, Zwolnione) oraz nazwa zainfekowanego pliku.
3. Aby wyświetlić więcej szczegółów dotyczących zainfekowanego pliku, wybierz plik.
  - W przypadku używania systemu Windows Mobile Professional lub Classic wybierz opcję **Pokaż szczegóły**.
  - Jeśli używasz systemu Windows Mobile Standard wybierz opcję **Menu→Pokaż szczegóły**.

## Przetwarzanie zainfekowanych plików

**Aby przetworzyć zainfekowane pliki, wykonaj następujące czynności:**

1. W widoku głównym otwórz menu **Ochrona przed wirusami**.
2. W menu *Ochrona przed wirusami* wybierz polecenie *Zainfekowane pliki*.
3. W widoku *Zainfekowane pliki* zaznacz zainfekowany plik do przetworzenia.
4. Można wybrać 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. Plik poddany kwarantannie jest zablokowany i nie może wyrządzić szkód na urządzeniu podczas działania aplikacji F-Secure Mobile Security.
  - **Zwolnij** — zwolnienie pliku z kwarantanny. Zwolnienie pliku powoduje jego odblokowanie. Użytkownik korzysta z takiego pliku na własne ryzyko.

W przypadku używania systemu Windows Mobile Professional lub Classic wybierz przycisk programowy.

Natomiast w systemie Windows Mobile Standard wybierz opcję **Menu**, a następnie wskaż odpowiednią czynność.

### 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 szybką zmianę poziomu zabezpieczeń zgodnie z potrzebami.

#### Wybieranie poziomu zabezpieczeń

**Aby wybrać poziom zabezpieczeń, wykonaj następujące czynności:**

1. W widoku głównym otwórz menu **Zapora**.
2. W menu Zapora wybierz polecenie **Ustawienia**.
3. Ustaw jeden z następujących poziomów 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 **Edytuj reguły niestandardowe**, gdy wybrany jest **Niestandardowy** poziom zabezpieczeń.

### 4. Ochrona poufnych informacji

Funkcja zabezpieczenia przed kradzieżą pomaga chronić urządzenie i przechowywane na nim dane przed niewłaściwym użyciem w przypadku kradzieży urządzenia.



*Kartę pamięci można łatwo wyjąć z urządzenia, dlatego należy przechowywać poufne informacje w pamięci urządzenia.*

#### Zabezpieczenia Kod

Kod zabezpieczeń pozwala zdalnie zlokalizować, zablokować lub wyczyścić urządzenie.

Kod zabezpieczeń musi zawierać co najmniej 8 znaków. Kod powinien być łatwy do zapamiętania, ale trudny do odgadnięcia. Przechowuj ten kod w bezpiecznym miejscu.

#### Zdalne rozwiązanie Anti-Theft

Za pomocą funkcji lokalizatora można wysłać wiadomość SMS na zgubione urządzenie, aby je zlokalizować.

Blokada zdalna pozwala zablokować urządzenie na odległość przez wysłanie na nie utworzonej przez siebie wiadomości SMS. Do używania blokady zdalnej wymagane jest włączenie funkcji blokady urządzenia.

Zdalne czyszczenie pozwala wyczyścić urządzenie na odległość przez wysłanie na nie utworzonej przez siebie wiadomości SMS. Wyczyszczenie urządzenia powoduje usunięcie wszystkich zapisanych na nim danych.

**Aby skonfigurować funkcje zdalnego blokowania i czyszczenia, wykonaj następujące czynności:**

1. W widoku głównym otwórz menu **Zabezpieczenie przed kradzieżą**.
2. W menu Zabezpieczenie przed kradzieżą wybierz polecenie **Ustawienia**.
3. Wybierz funkcje, które chcesz włączyć:
  - Jeśli chcesz uzyskać możliwość zdalnego lokalizowania urządzenia, wybierz opcję **Włącz lokalizator**.
  - Jeśli chcesz uzyskać możliwość zdalnego wyczyszczenia urządzenia, wybierz opcję **Włącz zdalne czyszczenie**.
  - Jeśli chcesz uzyskać możliwość zdalnego zablokowania urządzenia, wybierz opcję **Włącz blokadę zdalną**.



*Blokadę zdalną można zastosować tylko wtedy, gdy funkcje blokady urządzenia są włączone.*

4. Wprowadź i potwierdź swój **Kod zabezpieczeń**.

**Aby zdalnie zlokalizować, zablokować lub wyczyścić urządzenie, wykonaj następujące czynności:**

- W celu zlokalizowania urządzenia wyślij na nie wiadomość SMS o następującej treści:  
#LOCATE#<kod zabezpieczeń> (na przykład: #locate#12345678)
- W celu zablokowania urządzenia wyślij na nie wiadomość SMS o następującej treści:  
#LOCK#<kod zabezpieczeń> (na przykład: #lock#12345678)
- W celu wyczyszczenia urządzenia wyślij na nie wiadomość SMS o następującej treści:  
#WIPE#<kod zabezpieczeń> (na przykład: #wipe#12345678)

#### Alert SMS

Jeśli w urządzeniu zostanie zmieniona karta SIM, zabezpieczenie przed kradzieżą może wysłać odpowiedni alert. Aby włączyć funkcję alertów SMS, wybierz ustawienie **Wyślij alert SMS po zmianie karty SIM** i określ numer telefonu, na który ma zostać wysłana wiadomość SMS w przypadku zmiany karty SIM w urządzeniu.

## 5. Ochrona podczas przeglądania sieci Web

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

Za pomocą funkcji Ochrona przeglądania sprawdzane są witryny internetowe otwierane w przeglądarce Internet Explorer. Funkcja Ochrona przeglądania jest automatycznie włączana po aktywowaniu produktu F-Secure Mobile Security, jeśli program Internet Explorer jest ustawiony jako domyślna przeglądarka. Funkcja Ochrona przeglądania nie zapewnia bezpiecznego korzystania z Internetu w przypadku używania przeglądarek innych firm.

**Aby skonfigurować funkcję Ochrona przeglądania, wykonaj następujące czynności:**

1. W widoku głównym otwórz opcję **Ochrona przeglądania**.
2. W menu Ochrona przeglądania wybierz polecenie **Ustawienia**.
3. Aby włączyć tę funkcję, wybierz opcję **Włącz ochronę przeglądania**.

4. W polu **Sieć do użycia**, czy funkcja Ochrona przeglądania ma być aktywna przez cały czas, czy tylko podczas przeglądania Internetu przy użyciu sieci swojego operatora:
  - Wybierz ustawienie **Tylko mój operator**, aby używać funkcji Ochrona przeglądania tylko podczas korzystania z sieci operatora.
  - Wybierz ustawienie **Wszyscy operatorzy**, aby opcja przeglądania była włączona w podróży, gdy nie korzystasz z sieci swojego operatora.

## 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.

### Aktualizacje wersji

Aplikację i bazę danych definicji wirusów można też zaktualizować ręcznie:

1. W widoku głównym wybierz pozycję **Menu→Aktualizuj**.
2. Wybierz przycisk **Tak**, aby potwierdzić zamiar pobrania najnowszej aktualizacji.
3. Jeśli jest dostępna nowa wersja aplikacji, wybierz opcję **Tak**, gdy pojawia się monit o jej o pobranie.
4. Po zakończeniu aktualizacji wybierz przycisk **Tak**, aby przeskanować urządzenie w poszukiwaniu wirusów. Więcej informacji można znaleźć w części „*Skanowanie w poszukiwaniu wirusów*”.

## Więcej informacji

Więcej informacji można znaleźć w podręczniku użytkownika produktu (tylko w języku angielskim) dostępnym do pobrania z witryny <http://mobile.f-secure.com/>.

## Pomoc techniczna

W razie pytań dotyczących aplikacji, które nie zostały ujęte w podręcznikach ani w usługach online (dostępnych w witrynie <http://mobile.f-secure.com/>), 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 błędy 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 jakichkolwiek urządzeń (elektronicznych czy mechanicznych), w jakimkolwiek celu, bez wyraźnej pisemnej zgody firmy F-Secure Corporation.

Ten produkt może być objęty jednym lub większą liczbą patentów firmy F-Secure, w tym następującymi:

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

Copyright © 2010 F-Secure Corporation. Wszelkie prawa zastrzeżone.

