

F-Secure Mobile Security™ for Windows Mobile

1. 安裝和啟動

舊版本 若已安裝 F-Secure Mobile Security 的舊版本，則須將其關閉。安裝時將自動移除舊版本。

安裝 **安裝步驟：**



1. 傳輸 .cab 安裝檔案至裝置。
2. 在裝置的「檔案總管」中尋找和選擇 .cab 檔案。
3. 選擇**是**以允許安裝（若提示執行該動作）。
4. 選擇**是**以同意授權條款和條件。
5. 安裝應用程式後，將提示您重新啟動裝置。選擇 **是**。
6. 安裝準備就緒後，必須啟動產品。如果未啟動產品，則產品不會保護您的裝置。

啟動 **啟動步驟：**

1. 安裝 F-Secure Mobile Security 後第一次開啟裝置時，選擇所顯示啟動通知上的**是**。
2. 選擇啟動類型：
 - 如果要開始試用期限，請選擇**免費試用**，並選擇**下一步**，或
 - 若要取得完整授權版，請選擇**訂閱編號**作為啟動類型，然後選擇**下一步**。輸入訂閱編號並選擇**下一步**。
3. 選擇**是**以連線至更新服務。本應用程式將連線至更新服務並提交您的訂閱編號。第一次更新時，本應用程式將下載最新病毒碼數據庫。
4. 下載完成後，將有訊息通知您註冊已成功且應用程式已啟動。選擇**確定**以完成啟動。
5. 啟動完成後，掃描裝置上的病毒以確保裝置未受感染。如需更多資訊，請參閱**病毒掃描**章節。

如果您的訂閱代碼有效，且您正在使用免費試用版的應用程式，請轉至**購買**功能表，並輸入訂閱代碼以啟動訂閱。

啟動產品 啟動 F-Secure Mobile Security 後，它將在每次開啟裝置時自動啟動。

1. 如果使用 Windows Mobile Professional 或 Classic，請選擇**啟動 程式**  **Mobile Security**。
如果使用 Windows Mobile Standard，請選擇**啟動**  **Mobile Security**。
2. 若提示執行病毒掃描，請選擇**是**。

2. 病毒掃描

即時掃描開啟後，F-Secure Mobile Security 在後台作業並自動掃描檔案。

1. 如果在即時掃描時發現病毒，電腦將顯示一則訊息。選擇**是**以檢視受感染檔案，或選擇**否**以關閉視圖。
2. 「感染」視圖包含裝置上受感染檔案的清單。清單上每個項目將顯示受感染檔案的狀態（已隔、已釋放）與名稱。
3. 請選擇受感染檔案以檢視更多相關詳細資料。
 - 如果使用 Windows Mobile Professional 或 Classic，請點選**顯示詳細資料**。
 - 如果使用 Windows Mobile Standard，請選擇**功能表顯示詳細資料**。

處理受感染檔案

處理受感染檔案的步驟：

1. 在主視圖中開啟**病毒防護**。
2. 在**病毒防護**功能表中選擇受感染檔案。
3. 在**受感染檔案**視圖中，選擇要處理的受感染檔案。
4. 選擇以下一個動作：
 - **刪除** - 刪除受感染的檔案。建議使用此選項。
該檔案將從裝置中完全移除。
 - **隔離** - 隔離尚未隔離的受感染檔案。F-Secure Mobile Security 開啟時，電腦將鎖定隔離的檔案，使其無法損壞您的裝置。
 - **釋放** - 釋放隔離的檔案。如果釋放檔案，將不再鎖定該檔案。您自行承擔存取該檔案的風險。

如果使用 Windows Mobile Professional 或 Classic，請點選螢幕鍵盤。

如果使用 Windows Mobile Standard，請選擇**功能表**並選擇動作。

3. 防止未經授權的網路流量

F-Secure Mobile Security 的防火牆在後台隱密執行。它可以監視內送與外送的互聯網和網路流量，保護電腦免遭入侵嘗試的威脅。預定義的防火牆等級允許您根據需要即時變更保護等級。


選擇安全等級

選擇安全等級的步驟：

1. 在主視圖中開啟**防火牆**。
2. 在「防火牆」功能表中選擇**設定**。
3. 選擇以下一個防火牆等級：
 - **拒絕所有** - 停止所有網路流量。
 - **高** - 允許最常用的應用程式並封鎖所有內送流量。
 - **一般** - 允許所有外送連線並封鎖所有內送流量。
 - **允許所有** - 允許所有網路流量。
 - **自訂** - 根據自訂規則允許網路流量。要編輯自訂規則集，請選擇**編輯自訂規則**，此時需先選擇**自訂**安全等級。

4. 保護機密資訊

透過防竊功能，可在您的裝置失竊時確保該裝置及其儲存的數據不會遭到濫用。

 由於記憶卡可輕易移除，請將您的機密資訊儲存於裝置記憶體中。

安全代碼

可使用安全代碼來遠端鎖定或抹除裝置。

安全代碼最少需包含 8 個字元。請使用易記但難猜的代碼。請將安全代碼儲存於安全位置。

遠端鎖定和抹除

透過遠端鎖定功能，您可傳送您所建立的簡訊至裝置來遠端鎖定裝置。若要使用遠端鎖定功能，請開啟裝置鎖定。

透過遠端抹除功能，您可傳送您所建立的簡訊至裝置來遠端抹除裝置。抹除裝置後，會移除裝置上儲存的所有數據。

設定遠端鎖定和抹除的步驟：

1. 在主視圖中開啟**防竊**。
2. 在「防竊」功能表中選擇**設定**。
3. 若要遠端抹除裝置，請選擇**啟用遠端抹除**。
4. 若要遠端鎖定裝置，請選擇**啟用遠端鎖定**。

 僅在開啟裝置鎖定時才能啟用遠端鎖定。

5. 請輸入**安全代碼**並再次輸入以確認。

遠端鎖定或抹除裝置的步驟：

- 若要鎖定裝置，請發送以下簡訊至裝置：

#LOCK#< 安全代碼 > (例如： #lock#12345678)

- 若要抹除裝置，請發送以下簡訊至裝置：

#WIPE#< 安全代碼 > (例如： #wipe#12345678)

SIM 變更時發出簡訊警報

如果有人更換裝置中的 SIM 卡，防竊功能可提醒您。若要使用簡訊警報，請開啟設定，並指定更換裝置的 SIM 卡時，簡訊文字訊息需傳送到的電話號碼。

5. 使產品保持最新

自動更新 F-Secure Mobile Security 包含自動更新服務，這表示應用程式的病毒碼數據庫會定期更新。只有最新的病毒碼數據庫，才可保護您的裝置不受最新病毒攻擊。啟動產品後會使用自動更新。

本應用程式若要更新，互聯網連線必須處於活動狀態。連線互聯網時，應用程式會檢查病毒碼數據庫上一次更新的時間，並在必要時下載最新更新。

手動更新

您還可以手動更新應用程式：

1. 在主視圖中選擇**功能表更新**。
2. 選擇**是**以確認您要擷取最新更新。
3. 如果有新的應用程式更新可用，請在提示您下載時選擇**是**。
4. 更新完成後，請選擇**是**以掃描裝置中的病毒。如需更多資訊，請參閱**病毒掃描**章節。

如需更多資訊

如需更多資訊，請透過 <http://mobile.f-secure.com/> 下載產品的《使用者手冊》(英文版)。

技術支援

如果您對應用程式有疑問透過手冊或 <http://mobile.f-secure.com/> 線上服務均未能解答，您可聯絡本地 F-Secure 經銷商或直接聯絡 F-Secure Corporation。

免責聲明

「F-Secure」和三角形符號均為 F-Secure Corporation 的註冊商標，且 F-Secure 產品名稱和符號 / 標誌為 F-Secure Corporation 的商標或註冊商標。本文所提及的所有產品名稱皆為其各自公司的商標或註冊商標。F-Secure Corporation 對非本公司的其他商標和產品名稱不具有所有權。儘管 F-Secure Corporation 已盡力確保資訊準確，但對本文所述事實的任何錯誤或疏漏，F-Secure Corporation 概不負責。F-Secure Corporation 保留修改本文所述規格之權利，恕不預先通知。

除非另有說明，範例中所述公司、名稱和數據皆屬虛構。未經 F-Secure Corporation 書面許可，不得基於任何目的以任何電子或機械的形式或方式複製或傳輸本文的任何內容。

本產品受一項或多項 F-Secure 專利保護，包括：

GB2353372、GB2366691、GB2366692、GB2366693、GB2367933、GB2368233、GB2374260

版權所有 2009 F-Secure Corporation。保留所有權利

