

# F-Secure Mobile Security™ for Windows Mobile

## 1. 安装与激活

**旧版本** 如果已安装旧版 F-Secure Mobile Security，则必须将其关闭。安装过程中将自动删除旧版。

**安装** 若要安装，请执行以下操作：

1. 将 .cab 安装文件传送到您的装置。
2. 在装置的“资源管理器”中查找并选择 .cab 文件。
3. 如果系统提示安装，则选择**是**以允许安装。
4. 选择**是**以同意许可条款及条件。
5. 在安装应用程序后，会提示您重新启动您的装置。选择 **是**。
6. 安装准备就绪后需激活产品。如果未经激活，产品不会保护您的装置。

**激活** 若要开始激活，请执行以下操作：

1. 安装 F-Secure Mobile Security 后首次开启装置时，选择所显示激活通知上的**是**。
2. 选择激活类型：
  - 若要开始评估期限，请选择**免费评估**并选择**下一步**，或者
  - 若要获得完全授权的版本，请选择**订购编号**作为激活类型，并选择**下一步**。输入您的订购编号并选择**下一步**。
3. 选择**是**以连接至更新服务。将应用程序连接至更新服务，并提交您的订购编号。首次更新时，应用程序会下载最新的病毒定义数据库。
4. 下载完成时，系统将发送消息通知您已成功注册，且应用程序已激活。选择**确定**以完成激活。
5. 完成激活后，请对装置运行病毒扫描，以确保装置无病毒。有关详细信息，请参阅**病毒扫描**章节。

如果您有有效的订购代码且当前正在使用此应用程序的免费试用版，请转至**购买**菜单，并输入订购代码以激活订购。

**启动产品** 激活 F-Secure Mobile Security 后，产品会在每次开启装置时自动启动：

1. 如果您正在使用 Windows Mobile Professional 或 Classic，请选择**启动程序**  **Mobile Security**。  
如果您正在使用 Windows Mobile Standard，请选择**启动**  **Mobile Security**。
2. 如果提示您运行病毒扫描，请选择**是**。

## 2. 病毒扫描

开启实时扫描后，F-Secure Mobile Security 将在后台运行并自动扫描文件。

1. 如果在实时扫描时发现病毒，则会显示一条消息。选择**是**以查看受感染文件，或选择**否**以关闭视图。
2. 感染视图中包含装置上受感染文件的列表。将显示列表上各个项目的状态（已隔离或已释放）及受感染文件的名称。
3. 选择受感染文件以查看更多相关信息。
  - 如果您正在使用 Windows Mobile Professional 或 Classic，请单击**显示详细信息**。
  - 如果您正在使用 Windows Mobile Standard，请选择**菜单显示详细信息**。

### 处理受感染文件

若要处理受感染文件，请执行以下操作：

1. 在主视图中开启**病毒防护**。
2. 在**病毒防护**菜单中选择受感染文件。
3. 在**受感染文件**视图中选择要处理的受感染文件。
4. 选择以下一项操作：
  - **删除** - 删除受感染文件。建议使用此选项。文件将从装置中完全删除。
  - **隔离** - 隔离尚未隔离的受感染文件。在 F-Secure Mobile Security 开启时，将会锁定隔离的文件，使其无法损害您的装置。
  - **释放** - 释放隔离的文件。如果释放文件，则不会再锁定该文件。您需自行承担访问该文件的风险。

若您使用 Windows Mobile Professional 或 Classic，请单击软键。

如果您正在使用 Windows Mobile Standard，请选择**菜单**并选择操作。

## 3. 防止未经授权的网络流量

F-Secure Mobile Security 中的防火墙在后台隐密地工作。它会监视传入和传出的互联网和网络流量，以阻止入侵尝试。预定义的防火墙等级可允许您根据需要即时更改防护等级。


### 选择安全等级

若要选择安全等级，请执行以下操作：

1. 在主视图中打开**防火墙**。
2. 在“防火墙”菜单中选择**设置**。
3. 选择以下一种防火墙等级：
  - **拒绝全部** - 停止所有网络流量。
  - **高** - 允许最常用的应用程序，阻止所有传入流量。
  - **一般** - 允许所有传出连接，阻止所有传入流量。
  - **允许所有** - 允许所有网络流量。
  - **自定义** - 基于自定义规则允许网络流量。若要编辑自定义规则集，请在选择**自定义**安全等级后，选择**编辑自定义规则**。

## 4. 保护机密信息

通过防盗功能，您可确保装置被盗后，装置及其存储的数据不会遭到不当使用。

 **由于内存卡可以轻易地移除，因此请将机密信息存储在装置内存中。**

### 安全代码

可以使用安全代码来远程锁定或擦除装置。

安全代码至少需包含 8 个字符。使用易记但不易猜的代码。请将安全代码保存在安全的地方。


### 远程锁定和擦除

通过远程锁定功能，您可向装置发送您所创建的短信消息来远程锁定装置。若要使用远程锁定功能，请开启装置锁定。

通过远程擦除功能，您可向装置发送您所创建的短信消息来远程擦除装置。擦除装置时，将删除存储在装置上的所有数据。

**若要设置远程锁定和擦除，请执行以下操作：**

1. 在主视图中开启**防盗**。
2. 在“防盗”菜单中选择**设置**。
3. 如果要远程擦除装置，请选择**启用远程擦除**。
4. 如果要远程锁定装置，请选择**启用远程锁定**。

 **仅在开启装置锁定后才能启用远程锁定。**

5. 输入**安全代码**并再次键入以确认。

**若要远程锁定或擦除装置，请执行以下操作：**

- 若要锁定装置，请发送以下短信消息至装置：  
#LOCK#<安全代码>（例如：#lock#12345678）
- 若要擦除装置，请发送以下短信消息至装置：  
#WIPE#<安全代码>（例如：#wipe#12345678）

### 更换 SIM 时会发出短信警报

如果有人更换装置的 SIM 卡，防盗功能可通知您。若要使用短信警报，请开启设置，并指定更换装置的 SIM 卡时，短信需发送到的电话号码。

## 5. 保持产品处于最新状态

**自动更新** F-Secure Mobile Security 包括自动更新服务，这表示应用程序中的病毒定义数据库将定期更新。只有最新的病毒定义数据库，才可保护装置免遭最新的病毒感染。激活产品后，即可使用自动更新。

应用程序更新时，互联网连接必须处于活动状态。互联网连接可用时，应用程序会检查病毒定义数据库上次更新的时间，并在必要时下载新的更新程序。

**手动更新** 也可手动更新应用程序：

1. 在主视图中选择**菜单更新**。
2. 选择**是**以确认您要检索最新更新。
3. 如果有新的应用程序更新可用，请在系统提示下载时选择**是**。
4. 更新完成后，选择**是**以对您的装置进行病毒扫描。有关详细信息，请参阅**病毒扫描**章节。

### 如需更多详细信息

有关详细信息，请下载产品的《用户指南》（以英文提供），地址是 <http://mobile.f-secure.com/>。

### 技术支持

如果您无法在《指南》或在线服务 <http://mobile.f-secure.com/> 找到您的疑问的解答，您可以联系当地 F-Secure 分销商或直接联系 F-Secure 公司。

---

#### 免责声明

“F-Secure”和三角符号为 F-Secure Corporation 的注册商标，F-Secure 产品名称及符号 / 徽标均为 F-Secure Corporation 的商标或注册商标。本文所述的所有产品名称均为其各自公司的商标或注册商标。F-Secure Corporation 对于非本公司的商标和名称，不具有所有权。尽管 F-Secure Corporation 已尽力确保本文信息准确，但对其中所含错误或信息遗漏不承担责任。F-Secure Corporation 保留修改本文所述技术规范的权利，恕不另行通知。

除非另有说明，本文范例中提及的公司、名称和数据均为虚构。未经 F-Secure Corporation 书面同意，不得通过电子或机械形式，出于任何目的复制或散布本文的任何内容。

本产品可能受一项或多项 F-Secure 专利保护，包括：

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

版权所有 2009 F-Secure Corporation。保留所有权利

