ESET Mobile Security

Windows Mobile

安装手册和用户指南

ESET Mobile Security

全球客户服务：www.eset.eu/support
北美客户服务：www.eset.com/support

修订日期 14.10.2010

目录

1. ESET Mobile Security 的安装

1.1 系统最低要求

要安装用于 Windows Mobile 的 ESET Mobile Security，您的移动设备必须满足以下系统要求：

	系统最低要求
操作系统	Windows Mobile 5.0 及更高版本
处理器	200 MHz
内存	16 MB
可用空间	2.5 MB

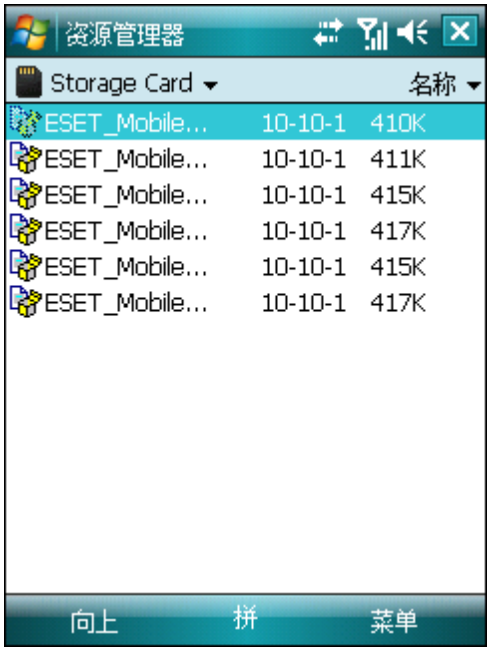
1.2 安装

安装前保存所有打开的文档并退出所有运行的应用程序。您可以在设备上直接安装 ESET Mobile Security 或使用计算机来安装它。

成功安装后，通过遵循产品激活 5 部分中的步骤激活 ESET Mobile Security。

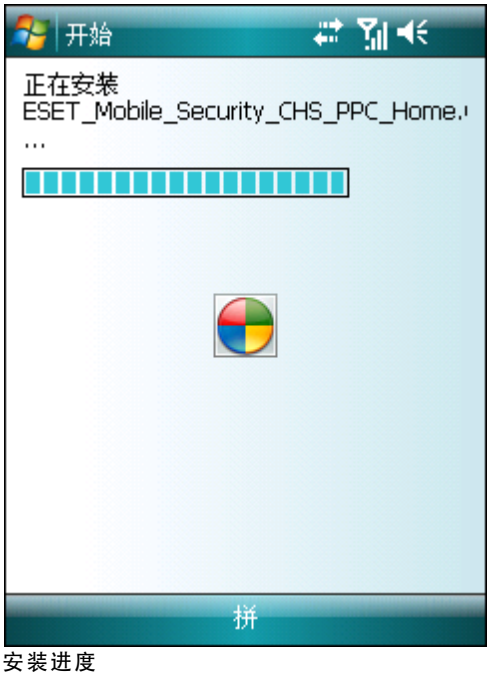
1.2.1 在设备上安装

要直接在设备上安装 ESET Mobile Security，则通过 Wi-Fi、蓝牙文件传输或电子邮件附件将 .cab 安装文件下载到设备。转至开始 > 程序 > 资源管理器来查找该文件。点击该文件以启动安装程序，然后遵循安装向导中的提示。



安装 **ESET Mobile Security**

注意： Windows Mobile 用户界面随设备型号的不同而不同。安装文件可能出现在设备的不同菜单或文件夹中。

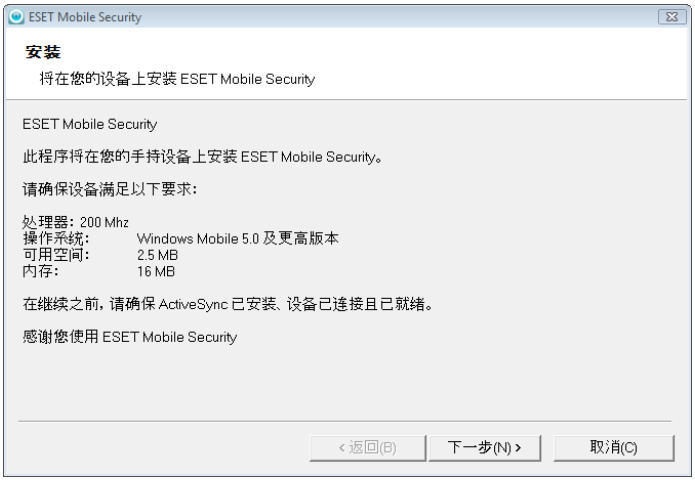


安装进度

安装后，可以修改程序设置。但是，默认配置可对恶意程序提供最高级别的防护。

1.2.2 使用计算机安装

要使用计算机安装 ESET Mobile Security，请通过 ActiveSync（在 Windows XP 中）或 Windows 移动设备中心（在 Windows 7 和 Vista 中）将移动设备连接到计算机。设备识别以后，运行下载的安装包（exe 文件）并遵循安装向导中的指示。



在计算机上启动安装程序

然后遵循移动设备上的提示。

1.3 卸载

要从移动设备上卸载 ESET Mobile Security，请点击开始 > 设置、点击系统选项卡，然后点击删除程序图标。

注意： Windows Mobile 用户界面随设备型号的不同而不同。这些选项在您的设备上可能稍有不同。

删除 **ESET Mobile Security**

选择 ESET Mobile Security 并点击删除。 提示确认卸载时点击是。

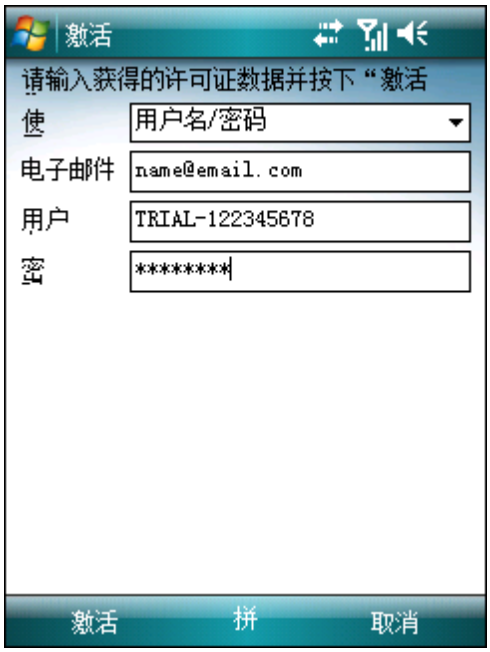
删除 **ESET Mobile Security**

2. 产品激活

主 ESET Mobile Security 窗口（开始 > 程序 > **ESET Mobile Security**）是本手册中所有指示的开始点。

主 **ESET Mobile Security** 窗口

成功安装之后，必须激活 ESET Mobile Security。如果未提示您激活产品，请点击菜单 > 激活。



程序激活

有两种激活方法；适用于您的方法取决于您获取 ESET Mobile Security 产品的方式。

2.1 使用登录名和密码激活

如果您从经销商处购得产品，则会随产品一起收到一个登录名和密码。选择用户名/密码选项，在登录名和密码字段输入收到的信息。在电子邮件字段输入当前联系人地址。点击激活完成激活。

2.2 使用激活码激活

如果您随新设备一起（或者作为套装产品）购买 ESET Mobile Security，产品会随附一个激活码。选择激活码选项并在密钥字段输入您收到的信息，以及在电子邮件字段输入当前联系人地址。点击激活完成激活。 您的新验证数据（登录名和密码）将自动替换激活码并被发送到您指定的电子邮件地址。

在这两种情况下，您都会收到有关产品成功激活的确认电子邮件。

每次激活只在固定的时间段内有效。激活过期后，需要更新程序的许可证（程序会提前向您发出通知）。

注意： 在激活期间，设备必须连接至 Internet。将下载少量数据。移动服务提供商会依据服务协议收取相应的传输费用。

3. 更新

默认情况下，ESET Mobile Security 与更新任务一起安装，以确保程序得到定期更新。您也可以手动执行更新。

安装后，建议第一次时进行手动更新。要进行此操作，请点击操作 > 更新。

3.1 设置

要配置更新设置，请点击菜单 > 设置 > 更新。

Internet 更新选项启用或禁用自动更新。

您可以指定从其下载更新的更新服务器（建议保留默认设置 updmobile.eset.com）。

要设置自动更新的时间间隔，请使用自动更新选项。

更新设置

注意： 为了防止不必要的带宽使用量，病毒库更新根据需要在添加新威胁时发布。虽然病毒库更新在您的许可证有效期内是免费的，但移动设备提供商可能对数据传输收取费用。

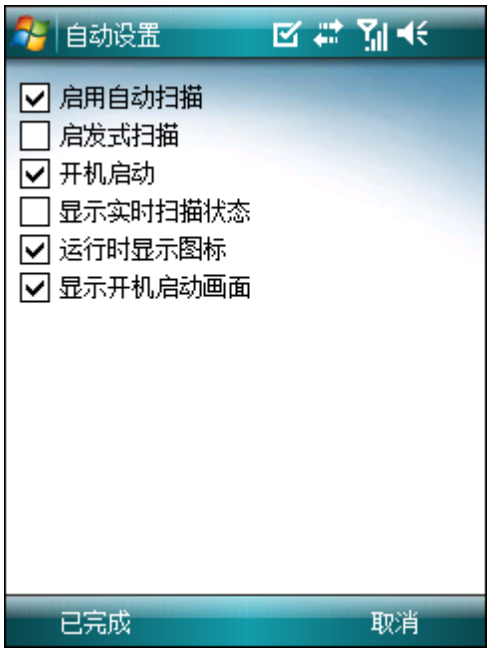
4. 自动扫描程序

自动扫描程序实时检查您与之交互的文件。运行、打开或保存文件时会自动检查威胁。在对文件进行任何操作之前先进行扫描，使用默认设置确保最大程度的防护。自动扫描程序在系统启动时自动启动。

4.1 设置

点击菜单 > 设置 > 自动以启用或禁用下列选项：

- 启用自动扫描 - 如果已启用，则自动扫描程序在后台运行。
- 启发式扫描 - 选择该选项可应用启发式扫描技术。启发式扫描通过分析代码和识别典型病毒行为，主动识别病毒库还未检测到的新恶意软件。其缺点是需要额外的时间来完成扫描。
- 重新启动之后运行 - 如果已选择，自动扫描程序将在设备重新启动后自动启动。
- 显示活动状态的扫描 - 选择该选项以在扫描正在进行时在右下角显示扫描状态。
- 运行时显示图标 - 显示自动扫描设置的快速访问图标（在 Windows Mobile 开始 屏幕的右下角）。
- 显示开机启动画面 - 此选项允许您关闭在设备启动期间显示的 ESET Mobile Security 初始屏幕。



自动扫描程序设置

5. 手动扫描程序

您可以使用手动扫描程序检查移动设备中是否存在威胁。默认状态下会扫描预定义的特定文件类型。

5.1 运行全盘扫描

全盘扫描检查内存、正在运行的进程及其关联的动态链接库(DLL)， 以及内部和移动存储中的文件。

要运行全盘扫描，请点击操作 > 扫描 > 整个设备。

注意： 默认情况下不执行内存扫描。可以在菜单 > 设置 > 常规中启用它。

运行全盘扫描

程序首先扫描系统内存（包括正在运行的进程及其关联的DLL），然后扫描文件和文件夹。系统会短暂显示扫描的每个文件的完整路径和文件名。

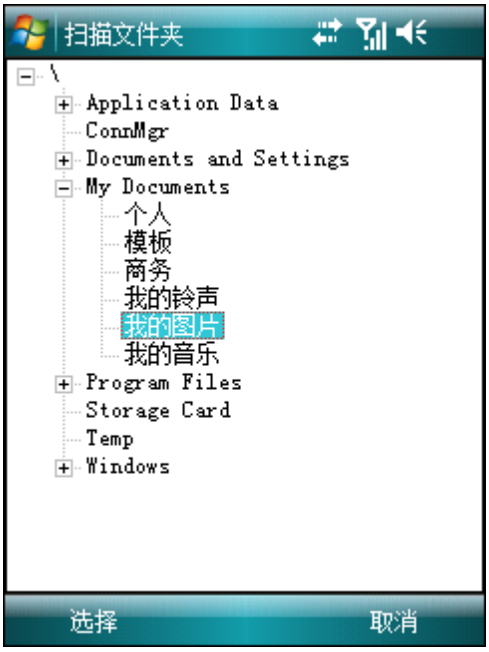
注意： 要中断正在进行的扫描，请点击操作 > 扫描 > 停止扫描。

5.2 扫描文件夹

要扫描设备上的特定文件夹，请点击操作 > 扫描 > 文件夹。

扫描文件夹

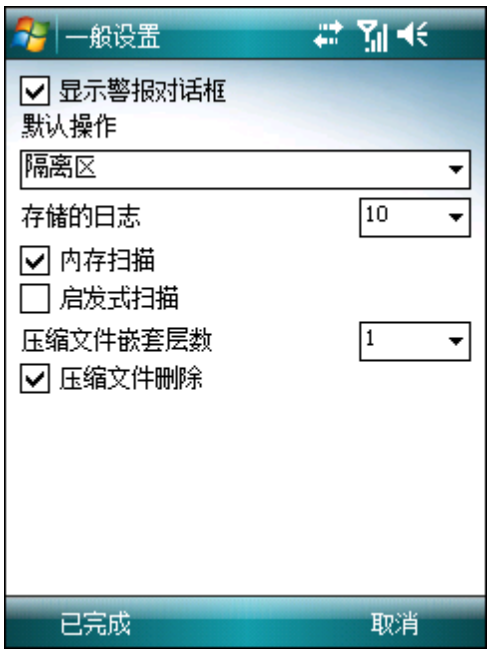
点击想要扫描的文件夹，然后点击选择。



选择要扫描的文件夹

5.3 常规设置

要修改扫描参数，请点击菜单 > 设置 > 常规。



常规设置

选择显示警报对话框选项可显示威胁警报通知。

可以指定当检测到被感染文件时将自动执行的默认操作。 可以从下列选项中进行选择：

- 隔离
- 删除
- 不操作 （不建议）

存储的日志选项允许您定义要存储在菜单 > 日志 > 扫描部分的最大日志数。

如果内存扫描已启用，则在实际文件扫描之前将自动扫描设备内存以查找恶意程序。

如果启发式扫描选项已启用，则 ESET Mobile Security 将使用启发式扫描技术。启发式扫描是基于算法的检测方法，它分析代码并搜索典型的病毒行为。其主要优点是能识别出当前病毒库无法识别的恶意软件。其缺点是需要额外的时间来完成扫描。

压缩文件嵌套选项允许您指定要扫描的嵌套压缩文件的深度。（数字越大，扫描得越深。）

如果压缩文件删除选项已启用，包含被感染对象的压缩文件（zip rar 和 jar）将自动删除。

5.4 扩展名设置

要在移动设备上指定要扫描的文件类型，请点击菜单 > 设置 > 扩展名。

将显示扩展名窗口，该窗口显示暴露给威胁的最常见的文件类型。选择想要扫描的文件类型或取消选择要排除扫描的扩展名。 如果启用压缩文件选项，将扫描所有支持的压缩文件（zip rar 和 jar）。

要扫描所有文件，则取消选择检测的文件类型复选框。

扩展名设置

6. 发现威胁

如果发现威胁，ESET Mobile Security 将提示您执行操作。

威胁警报对话框

建议您选择删除。如果选择隔离，该文件将从其原始位置移动到隔离区。如果选择忽略，系统将不进行任何操作，被感染文件将仍然留在您的移动设备中。

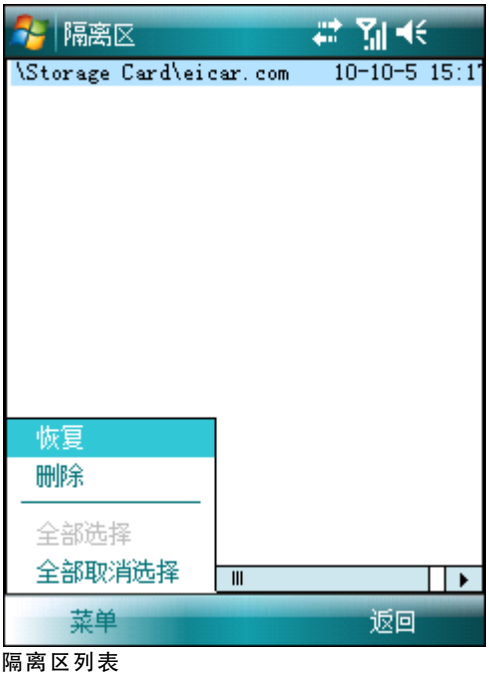
如果在压缩文件（例如 .zip 文件）中检测到渗透，警报窗口中的删除压缩文件选项将变得可用。同时选择该选项和删除选项可删除所有压缩文件。

如果禁用显示警报对话框选项，当前扫描期间将不显示任何警报窗口（如果要对将来的所有扫描禁用警报，请参见常规设置 9）。

6.1 隔离区

隔离区的主要任务是安全储存被感染文件。隔离文件的前提是文件出现以下情况：无法清除、不安全或被建议删除，或被 ESET Mobile Security 错误检测。

可在日志中查看存储在隔离区文件夹中的文件，同时显示隔离的日期和时间以及被感染文件的原始位置。要打开隔离区，请点击菜单 > 查看 > 隔离区。



隔离区列表

您可以通过点击菜单 > 恢复来恢复隔离的文件（每个文件都会被恢复到其原始位置）。如果想要永久删除文件，则点击菜单 > 删除。

7. 手机防盗

Anti-Theft 功能保护您的手机免遭未授权访问。

如果您的电话丢失或被盗，而且 SIM 卡被新（不被信任的）卡所替换，将有一条警报 短信 秘密发送到用户定义的特定电话号码。此邮件将包含当前插入的 SIM 卡的电话号码、IMSI（国际移动用户识别码）号码和电话的 IMEI（国际移动设备识别码）号码。未授权的用户不会意识到此邮件已被发送，因为它将自动从 已发送 文件夹中删除。

要擦除存储在设备和所有当前插入的可移动磁盘上的所有数据（联系人、邮件、应用程序），可以将一条远程擦除 SMS 发送至未授权用户的移动号码，格式如下：
#RC# DS 密码
其中*密码*是在菜单 > 设置 > 密码中设置的自己的密码。

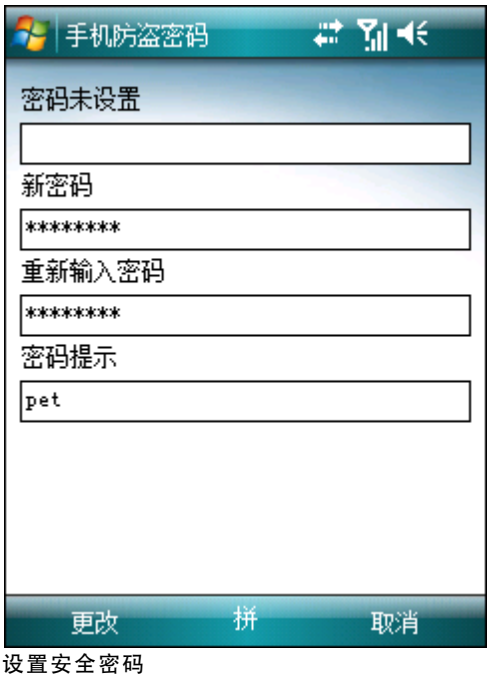
7.1 设置

首先，在菜单 > 设置 > 密码中设置密码。此密码用于：
- 将远程擦除 SMS 发送到您的设备
- 访问您的设备上的 Anti-Theft 设置
- 从设备上卸载 ESET Mobile Security。

要设置新密码，在新密码和重新输入密码字段中输入密码。提醒选项（如果已设置）在您忘记密码时显示提示。

要更改现有密码，首先输入当前密码，然后输入新密码。

重要信息： 请仔细选择密码，因为在从设备上卸载 ESET Mobile Security 时将需要该密码。



设置安全密码

要访问 Anti-Theft 设置，请点击菜单 > 设置 > **Anti-Theft** 并输入密码。

要禁用插入的 SIM 卡（和可能发送警报 SMS）的自动检查，请取消选择启用 **SIM** 匹配选项。

如果当前插在移动设备中的 SIM 卡是您希望保存为信任的卡，则选中当前 **SIM** 可信复选框，SIM 将保存到信任的 SIM 列表（信任的 **SIM** 选项卡）。**SIM** 别名文本框将自动填写为 IMSI 号码。

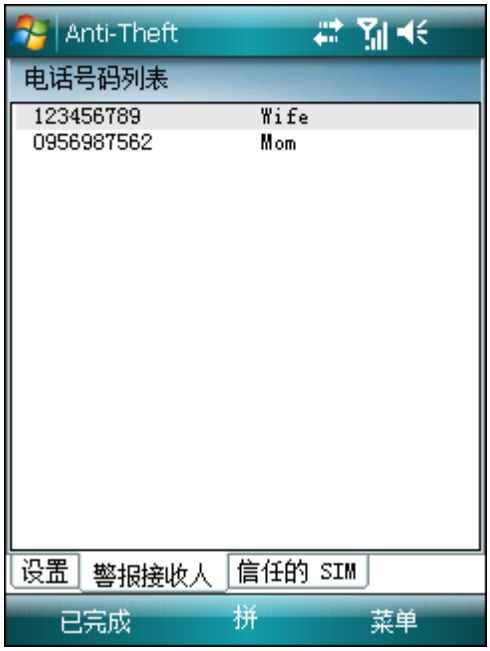
如果您使用多个 SIM 卡，则可能想要通过修改其 **SIM** 别名（例如，*办公室* *家庭*等）来进行区分。

在警报 **SMS** 中，可以修改在将不信任的 SIM 卡插入设备后将发送到预定义的号码的文本消息。

Anti-Theft 设置

警报接收人选项卡显示在将不信任的 SIM 卡插入设备后将接收警报 SMS 的预定义的号码列表。要添加新号码，请点击菜单 > 添加。要从联系人列表添加号码，请点击菜单 > 添加联系人。

注意： 电话号码必须包括国际区号，然后是实际号码（例如，+16105552000）。



预定义的电话号码列表

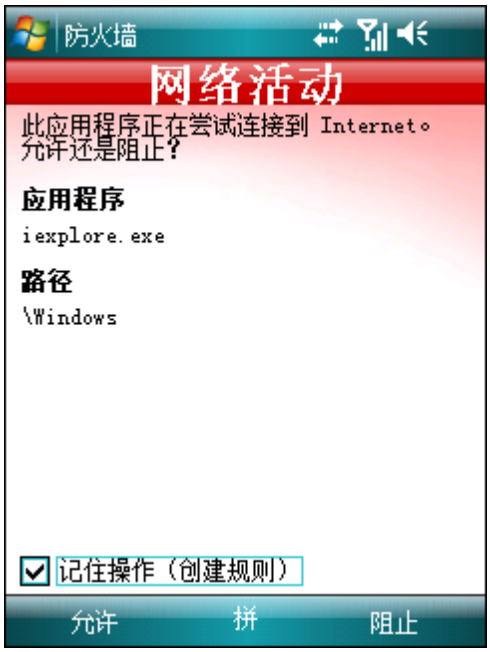
信任的 **SIM** 选项卡显示信任的 SIM 卡列表。每个条目包括 SIM 别名（左列）和 IMSI 号码（右列）。

要从列表中除去某个 SIM，则选择该 SIM 并点击菜单 > 删除。

信任的 **SIM** 列表

8. 防火墙

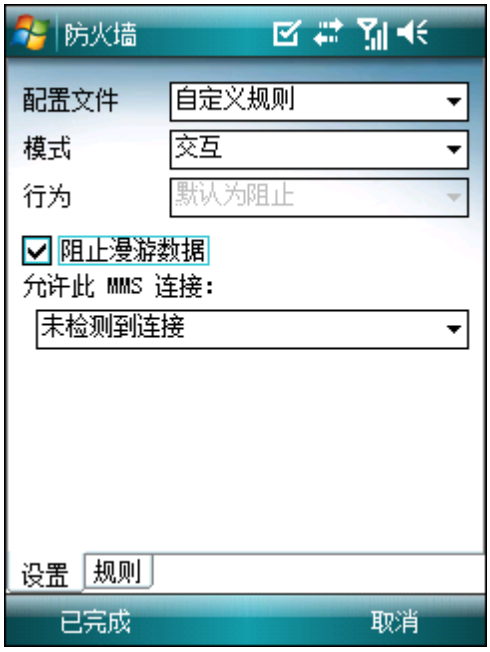
通过基于过滤规则允许或拒绝个别连接，防火墙控制所有入站和出站网络流量。



防火墙警报

8.1 设置

要修改防火墙设置，请点击菜单 > 设置 > 防火墙。



防火墙设置

可以从下列配置文件中进行选择：

- 全部允许 - 允许所有网络流量
- 全部阻止 - 阻止所有网络流量
- 自定义规则 - 让您定义自己的过滤规则

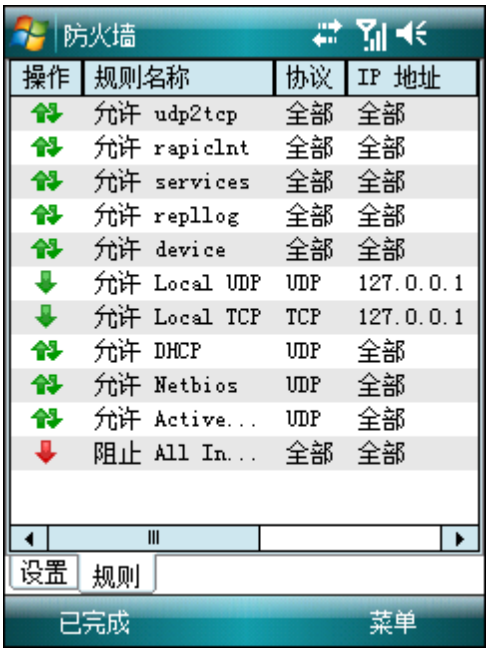
在自定义规则配置文件中，可以从两种过滤模式中进行选择：

- 自动 - 它适用于希望防火墙用起来简单、方便且无需定义规则的用户。此模式允许所有出站流量。对于入站流量，可以在行为选项中设置默认的操作（默认为允许或默认为阻止）。
- 交互 - 允许您自定义个人防火墙。当检测到无相应规则的通信时，将显示一个对话窗口，报告未知连接。该对话窗口将让您选择允许或阻止该通信以及创建规则。如果您选择创建规则，将来所有类似连接将根据该规则被允许或阻止。如果带有现有规则的应用程序被修改，则显示一个对话窗口，让您选择接受或拒绝此更改。现有规则将基于您的反应而修改。

阻止漫游数据 - 如果启用，ESET Mobile Security 会自动检测您的设备是否连接到漫游网络并阻止传入和传出的数据。此选项不阻止通过 Wi-Fi 或 GPRS 接收的数据。

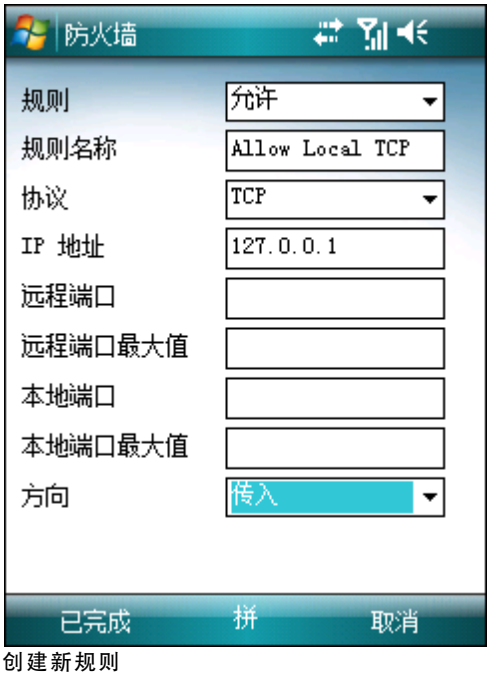
允许此 **MMS** 连接 - 选择用于接收漫游网络中的 MMS 邮件的连接。来自其他连接的 MMS 邮件将被 ESET Mobile Security 阻止。

在规则选项卡，可以编辑或删除现有过滤规则。



防火墙规则列表

要创建新规则，请点击菜单 > 添加，填写所有必填字段并点击完成。

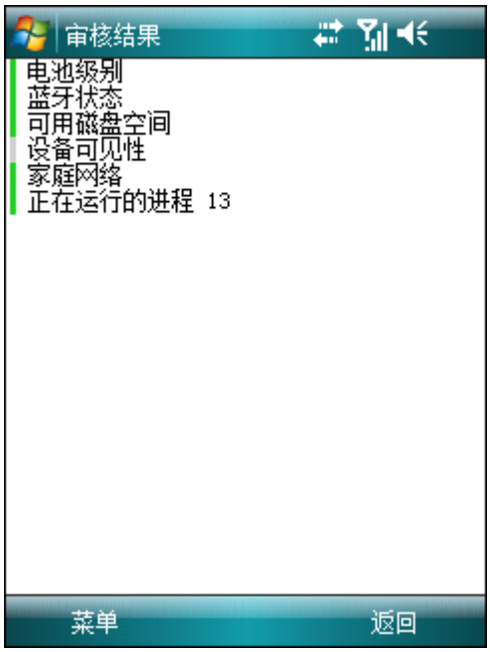


创建新规则

9. 系统检测

安全审核检查关于电池级别、蓝牙状态、可用磁盘空间等的电话状态。

要手动运行安全审核，请点击操作 > 系统检测。 将显示详细报告。

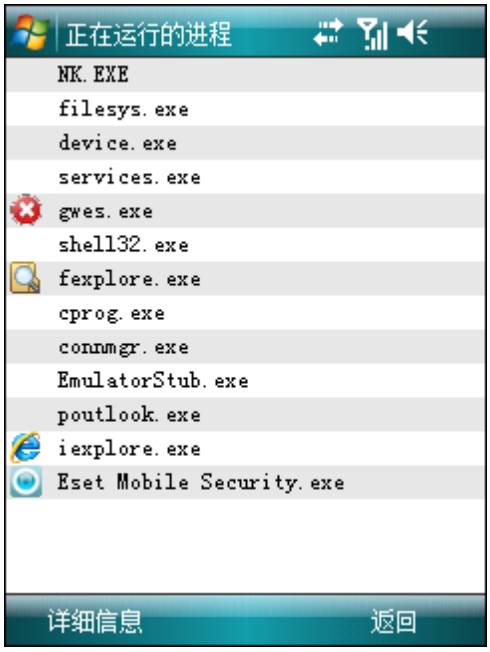


系统检测结果

每一项旁边的绿色表示该值超出阈值或该项没有出现安全风险。红色表示该值低于阈值或该项可能存在潜在安全风险。

如果蓝牙状态或设备可见性以红色突出显示，可以通过选择该项并点击菜单 > 修复来关闭其状态。

要查看每一项的详细信息，则选择该项并点击菜单 > 详细信息。



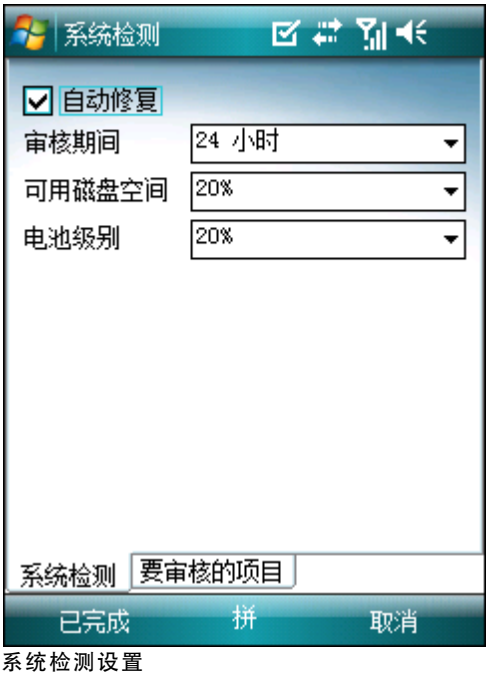
正在运行的进程

正在运行的进程选项显示正在设备上运行的所有进程的列表。

要查看进程详细信息（进程的完整路径名及其内存使用量），则选择该进程并点击详细信息。

9.1 设置

要修改系统检测参数，请点击菜单 > 设置 > 系统检测。



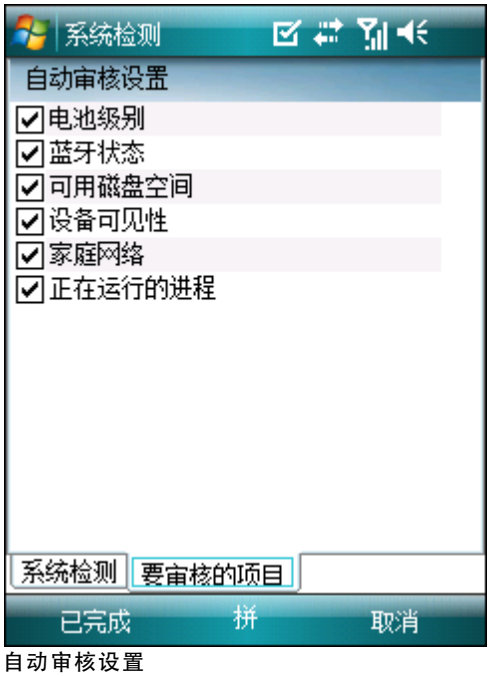
系统检测设置

如果自动修复选项已启用，ESET Mobile Security 将自动尝试修复具有风险的项目（例如，蓝牙状态、设备可见性）而无需用户交互。此设置仅应用于自动（计划的）审核。

审核周期选项允许您选择自动审核的执行频率。如果您想要禁用自动审核，请选择从不。

您可以调整阈值，可用磁盘空间和电池级别在该值将被视为低。

在要审核的项目选项卡，可以选择在自动（计划的）系统检测期间要检查的项目。



自动审核设置

10. 反垃圾邮件

反垃圾邮件阻止发送到移动设备的未经请求的 SMS 和 MMS 邮件。

未经请求的邮件通常包括来自移动电话服务提供商的广告或来自未知或未指定用户的邮件。

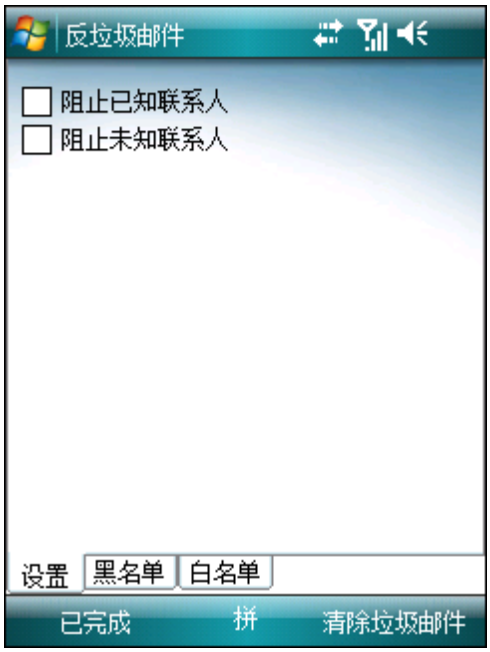
10.1 设置

点击菜单 > 查看 > 统计信息可以查看有关已接收邮件和已阻止邮件的统计信息。

在反垃圾邮件设置中（菜单 > 设置 > 反垃圾邮件），有以下过滤模式可用：

- 阻止未知联系人 - 启用该选项将只接受来自您的地址簿的联系人的邮件。
- 阻止已知联系人 - 启用该选项将只接受来自不包含在您的地址簿的发件人的邮件。
- 同时启用阻止未知联系人和阻止已知联系人来自动阻止所有传入的邮件。
- 同时禁用阻止未知联系人和阻止已知联系人来关闭反垃圾邮件。系统将接受所有传入的邮件。

注意： 白名单和黑名单的各项优先于这些选项（请参见白名单/黑名单 17 部分）。



反垃圾邮件设置

10.2 白名单/ 黑名单

黑名单是一个其所有邮件都将被阻止的电话号码列表。此处所列各项优先于反垃圾邮件设置（设置选项卡）中的所有选项。

白名单是一个其所有邮件都将被接受的电话号码列表。此处所列各项优先于反垃圾邮件设置（设置选项卡）中的所有选项。

黑名单

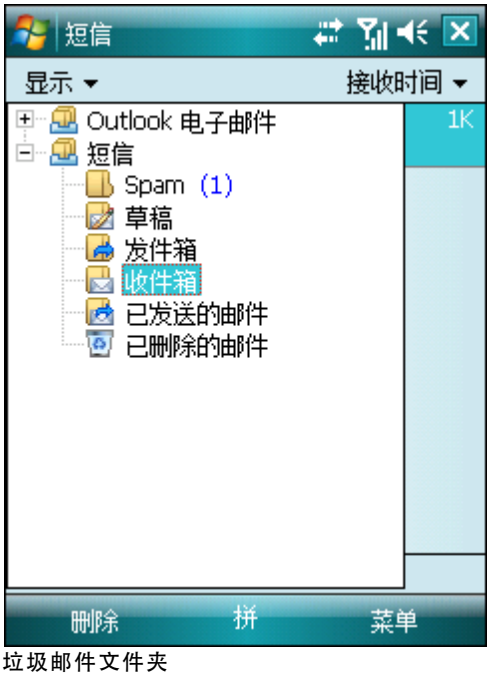
要将新号码添加到白名单/黑名单，请选择想要修改的名单的选项卡，并点击菜单 > 添加。要从联系人列表添加号码，请点击菜单 > 添加联系人。

警告: 向黑名单中添加号码/联系人将自动且无通知地把该发件人的邮件移至垃圾邮件文件夹。

10.3 查找垃圾邮件

垃圾邮件文件夹用于存储根据反垃圾邮件设置归类为垃圾邮件的被阻止的邮件。当收到第一条垃圾邮件时，自动创建该文件夹。要查找垃圾邮件文件夹并查看被阻止的邮件，请执行下列步骤：

1. 打开设备用于消息发送的程序，例如从开始菜单打开 Messaging
2. 点击文本消息（或 MMS，如果想要查找 MMS 垃圾邮件文件夹）
3. 点击菜单 > 转至 > 文件夹...（或智能手机上的菜单 > 文件夹 ）
4. 选择垃圾邮件文件夹。



垃圾邮件文件夹

10.4 删除垃圾邮件

要从移动设备上删除垃圾邮件，请遵循下面的步骤：

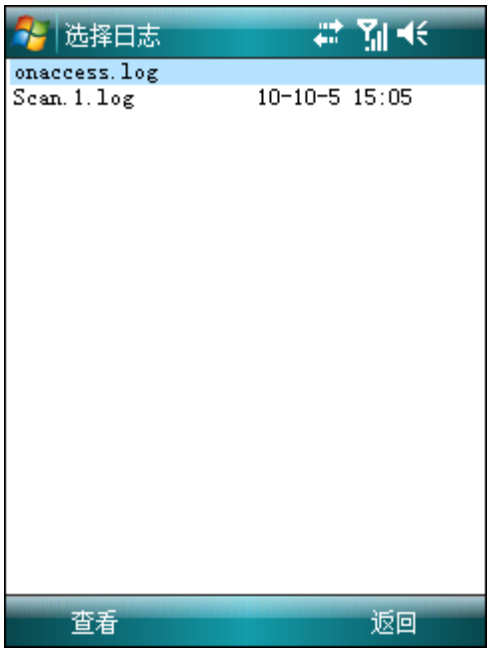
1. 从 ESET Mobile Security 主窗口点击菜单 > 设置 > 反垃圾邮件
2. 点击清除垃圾邮件
3. 点击是确认删除所有垃圾邮件。

删除垃圾邮件

11. 查看日志和统计信息

扫描日志部分（菜单 > 日志 > 扫描）包含提供有关已完成扫描任务的完整数据的日志。在每次成功手动扫描之后或当由自动扫描检测到威胁时，都会创建日志。所有被感染文件以红色突出显示。在每个日志条目的末尾，带有为什么该文件被包含在日志中的解释。

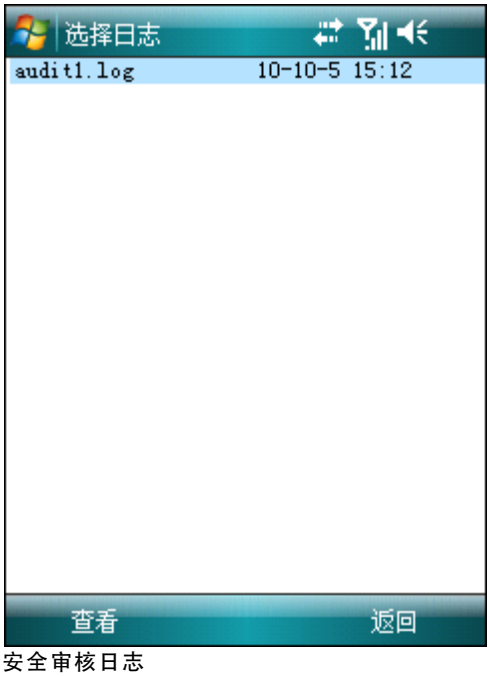
扫描日志包括：
- 日志文件名称（通常格式为 Scan.Number.log ）
- 事件的日期和时间
- 扫描的文件列表
- 扫描期间执行的操作或遇到的错误



扫描日志

安全审核日志部分（菜单 > 日志 > 安全审核）存储来自自动（计划的）审核和手动触发审核的全部安全审核结果。

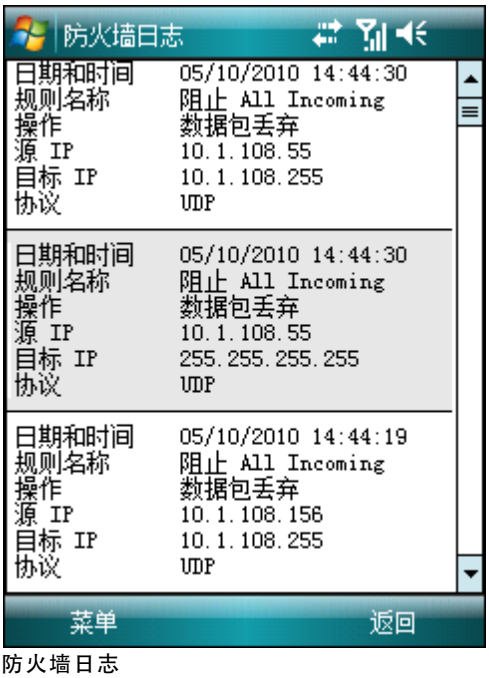
安全审核日志包括：
- 日志文件名称（格式为 auditNumber.log ）
- 审核的日期和时间
- 详细结果



安全审核日志

防火墙日志（菜单 > 日志 > 防火墙）包含关于被 ESET Mobile Security 阻止的防火墙事件的信息。在每次通过防火墙执行通信以后，日志将更新。新事件出现在日志的顶部。

防火墙日志包括：
- 事件的日期和时间
- 所用规则的名称
- 执行的操作（基于规则设置）
- 源 IP 地址
- 目标 IP 地址
- 所用协议



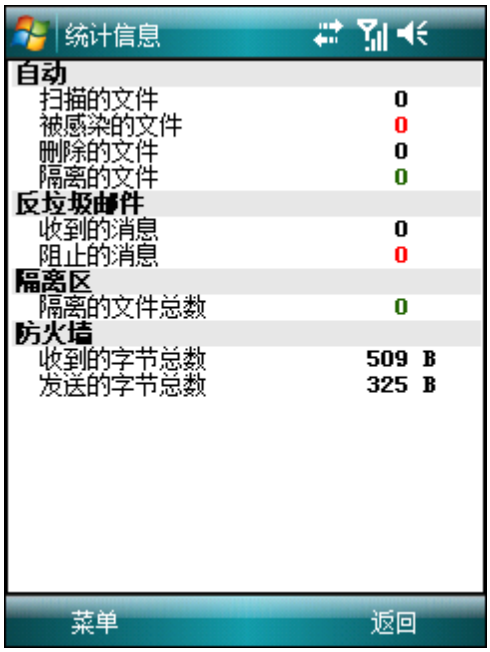
防火墙日志

统计信息屏幕（菜单 > 查看 > 统计信息）显示以下信息的摘要：

- 由自动扫描程序扫描的文件
- 收到的和阻止的邮件
- 隔离的文件
- 通过防火墙接收和发送的数据

如果想要重置当前统计信息，则点击菜单 > 重置计数器。

注意： 所有统计数据从设备最近一次重新启动开始计算。

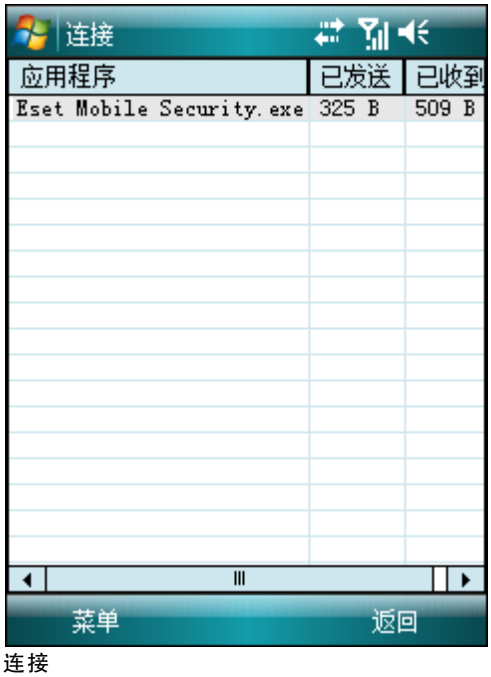


统计信息

连接部分（菜单 > 查看 > 连接）显示用于发送和接收数据的应用程序。

该信息包括：

- 进程的名称
- 发送的数据量
- 接收的数据量



连接

12. 故障排除和支持

12.1 故障排除

本节提供与 ESET Mobile Security 相关的常见问题的解决方法。

12.1.1 未成功的安装

在安装期间显示的错误消息的最常见原因是在设备上安装了 ESET Mobile Security 的错误版本。当从 *ESET 网站*下载安装文件时，请确保下载的是适用于您的设备的正确产品版本。

12.1.2 连接更新服务器失败

如果程序无法与更新服务器建立通讯，更新尝试则会失败，这时会显示该错误消息。

尝试下列解决方法：

1. 检查 Internet 连接 - 打开 Internet 浏览器并连接至 http://www.eset.com，确认您已连接到 Internet
2. 确认程序正使用正确的更新服务器 - 点击菜单 > 设置 > 更新，您应在更新服务器字段中看到 updmobile.eset.com。

12.1.3 下载文件超时

更新时 Internet 连接意外降速或中断。请稍后尝试重新运行更新。

12.1.4 缺少更新文件

如果您正尝试从更新文件 (esetav_wm.upd) 安装新的病毒库，则该文件必须出现在 ESET Mobile Security 安装文件夹 (\Program Files\ESET\ESET Mobile Security) 中。

12.1.5 病毒库文件已损坏

病毒库更新文件 (esetav_wm.upd) 已损坏。您需要替换该文件并重新运行更新。

12.2 技术支持

如需与 ESET Mobile Security 或其他任何 ESET 安全产品相关的行政协助或技术支持，我们的客户服务专家会为您提供帮助。要查找技术支持问题的解决方法，您可以做如下选择：

要查找最常见问题的解决方法，请访问 ESET 知识库，地址为：
http://kb.eset.com

该知识库包括丰富的有用信息用于解决最常见的问题，并带有分类和高级搜索。

要联系 ESET 的客户服务部门，请使用支持申请表，下载地址为：
http://eset.com/support/contact.php