

MOBILE SECURITY

Dành cho Android

Hướng dẫn sử dụng

(sử dụng cho phiên bản 3.0 và cao hơn)

Nhấp vào đây để tải phiên bản mới nhất của tài liệu này



© ESET, spol. s r.o.

ESET Mobile Security được phát triển bởi ESET, spol. s r.o.

Để biết thêm chi tiết, truy cập www.eset.com

Sản phẩm đã được đăng ký bản quyền. Không được sao chép bất cứ phần nào của tài liệu này, hoặc lưu trữ truy xuất trong hệ thống, chuyển đổi sang bất cứ định dạng nào hay thay đổi về ý nghĩa, điện tử, cơ khí, bản sao, ghi chép, sao chép hoặc bất cứ thứ gì khi chưa được phép từ tác giả. ESET, spol. s r.o có quyền thay đổi bất cứ mô tả ứng dụng phần mềm nào mà không cần báo trước.

Chăm sóc khách hàng: www.eset.com/support

Duyệt ngày 22/10/2014.

Mục lục

1. Giới thiệu.....	3
1.1 Có gì mới.....	3
1.2 Yêu cầu hệ thống.....	3
2. Cài đặt.....	4
2.1 Cài đặt từ trang web ESET.....	4
2.2 Cài đặt từ Google Play.....	4
2.3 Cài đặt từ Amazon.....	4
2.4 Hướng dẫn ban đầu.....	4
2.5 Gỡ bỏ.....	5
3. Bản quyền.....	6
4. Diệt virus.....	7
4.1 Quét tự động.....	7
4.2 Cách ly.....	8
4.3 Bỏ qua mối nguy hiểm.....	8
4.4 Lưu thông tin quét.....	8
4.5 Cấu hình nâng cao.....	8
5. Chống mất cắp.....	10
5.1 my.eset.com.....	10
5.2 Tinh chỉnh.....	10
5.3 Bảo vệ sim.....	10
5.3.1 Thêm vào sim tin cậy.....	10
5.4 Banned tin cậy.....	10
5.4.1 Thêm banned tin cậy.....	10
5.5 Cấu trúc lệnh cho tin nhắn.....	10
5.6 Chi tiết danh bạ.....	11
6. Tin nhắn và lọc cuộc gọi.....	12
6.1 Quy tắc.....	12
6.1.1 Thêm quy tắc mới.....	12
6.2 Lịch sử.....	13
7. Chống lừa đảo.....	14
7.1 Lịch sử.....	14
8. Tinh chỉnh độ bảo vệ.....	15
8.1 Kiểm soát thiết bị.....	15
8.2 Tinh chỉnh ứng dụng.....	15
9. Cấu hình.....	16
9.1 An toàn mật khẩu.....	16
10. Chăm sóc khách hàng.....	16

1. Giới thiệu

ESET Mobile Security là giải pháp toàn diện để bảo vệ an toàn cho thiết bị của bạn trước những mối đe dọa và lừa đảo, lọc các cuộc gọi tin nhắn không mong muốn, cho phép bạn kiểm soát thiết bị từ xa trong trường hợp mất cắp

1.1 Có gì mới?

Sau đây là những nâng cấp và cải tiến trong phiên bản ESET Mobile Security phiên bản 3:

- Tích hợp tính năng ESET Anti-Theft vào trang my.eset.com.
- Theo dõi vị trí- vị trí của thiết bị sẽ được hiển thị trên bản đồ.
- Chụp hình camera - tự động chụp hình camera trước và sau ngay khi thiết bị được chuyển sang chế độ mất cắp.
- Hiển thị tin nhắn lên màn hình- gửi 1 tin nhắn với nội dung được soạn sẵn đến thiết bị mất cắp.
- Khóa tự động- Thiết bị sẽ bị khóa ngay khi có những hành động nghi ngờ hoặc được chuyển sang chế độ mất cắp.
- Pin yếu- Khi điện thoại gần hết pin, ESET Mobile Security sẽ gửi vị trí thiết bị đến my.eset.com.
- Báo động- Điều khiển bật còi hú báo động từ my.eset.com nếu bạn nghi ngờ thiết bị đang ở gần.
- Thay đổi mật khẩu- Chủ động thay đổi mật khẩu tại my.eset.com trong trường hợp bạn quên mất.
- Xóa dữ liệu từ xa- Xóa toàn bộ dữ liệu quan trọng trong thiết bị từ my.eset.com.
- Bỏ qua nguy hiểm – Tạo danh sách loại trừ các mối nguy hiểm trong lần quét kế tiếp.
- Quét khi sạc- Tự động quét khi thiết bị ở trạng thái rảnh và được cắm sạc.

1.2 Yêu cầu hệ thống

Để cài đặt ESET Mobile Security, thiết bị Android của bạn phải đạt tối thiểu những yêu cầu sau:

Hệ điều hành: Android 2.3 (Gingerbread) và độ phân giải màn hình: tối thiểu 240x320 px, khuyến khích 320x 480 px

CPU: 500 MHz (ARM7+)

CPU: 500 Mhz (ARM7+)

RAM: 128 MB

Dung lượng dư ổ cứng: 20MB

Kết nối internet

LƯU Ý: thiết bị sử dụng 2 sim hoặc root sẽ không được hỗ trợ.
Một vài tính năng (như chống trộm, gửi tin nhắn và lọc cuộc gọi) sẽ không dùng được trên máy tính bảng mà không hỗ trợ gọi hoặc gửi tin nhắn

2. Cài đặt

Để cài đặt ESET Mobile Security, sử dụng một trong những phương pháp sau

LƯU Ý: Nếu bạn đã có sẵn Tên đăng nhập và Mật khẩu hoặc mã kích hoạt được cung cấp bởi ESET, vui lòng tải ESET Mobile Security từ trang web ESET

2.1 Cài đặt từ website ESET

Tải ESET Mobile Security bằng cách quét mã QR bên dưới, sử dụng thiết bị và ứng dụng QR Droid hay Barcode Scanner để quét:



Hoặc theo cách khác, bạn có thể tải gói cài đặt APK ESET Mobile Security trên máy tính :

1. Tải tập tin từ [trang web ESET](#).
2. Sao chép tập tin sang thiết bị thông qua Bluetooth hoặc USB.
3. Chọn biểu tượng  trên màn hình chủ Android, hoặc vào **Home > Menu** và chọn **Setting > Applications**. Đảm bảo rằng ứng dụng từ **nguồn không xác định** được cho phép trên thiết bị của bạn.
4. Xác định tập tin APK được sử dụng bởi ứng dụng ASTRO File Manager hoặc ES File Explorer.
5. Mở tập tin và chọn **Install**. Khi ứng dụng đã được cài đặt, chọn **Open**

2.2 Cài đặt từ Google Play

Mở ứng dụng Google Play Store trên thiết bị Android của bạn và tìm “ESET Mobile Security” (hoặc chỉ Eset)

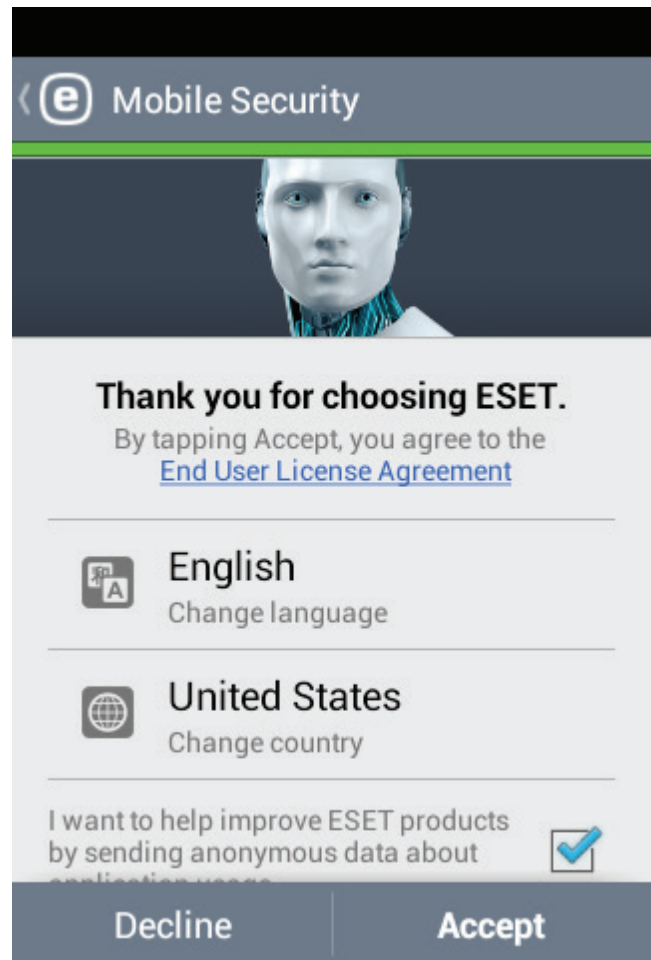
Hoặc, bạn có thể cài đặt chương trình bằng cách quét mã QR bên dưới bằng ứng dụng QR Droid hoặc Barcode Scanner:



2.3 Cài đặt từ Amazon

Mở ứng dụng Amazon trên thiết bị Android của bạn và tìm “ESET Mobile Security” (hoặc chỉ Eset)

2.4 Hướng dẫn ban đầu

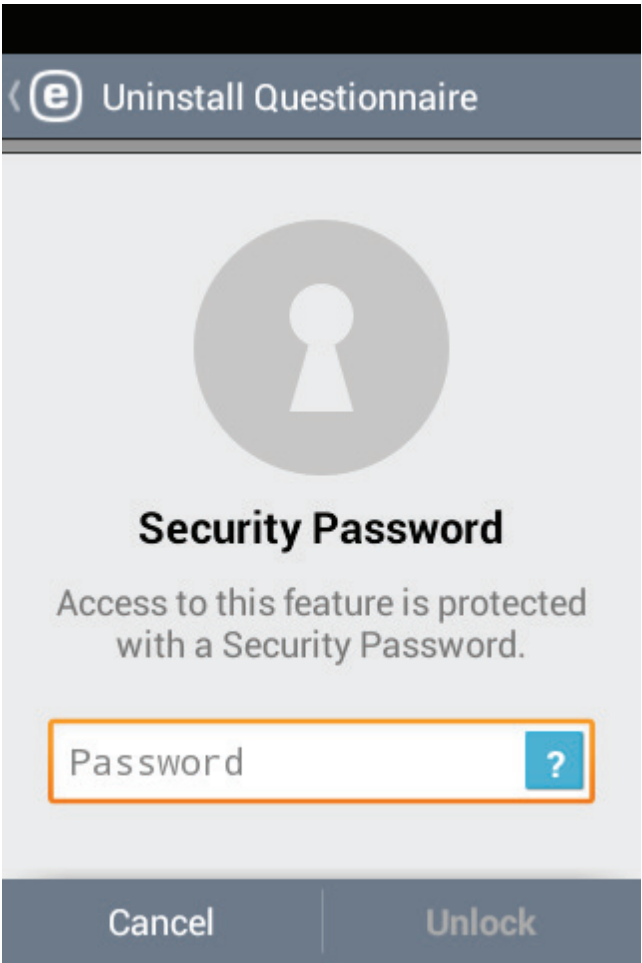


Khi ứng dụng đã được cài đặt trên thiết bị, làm theo gợi ý trên màn hình hướng dẫn:

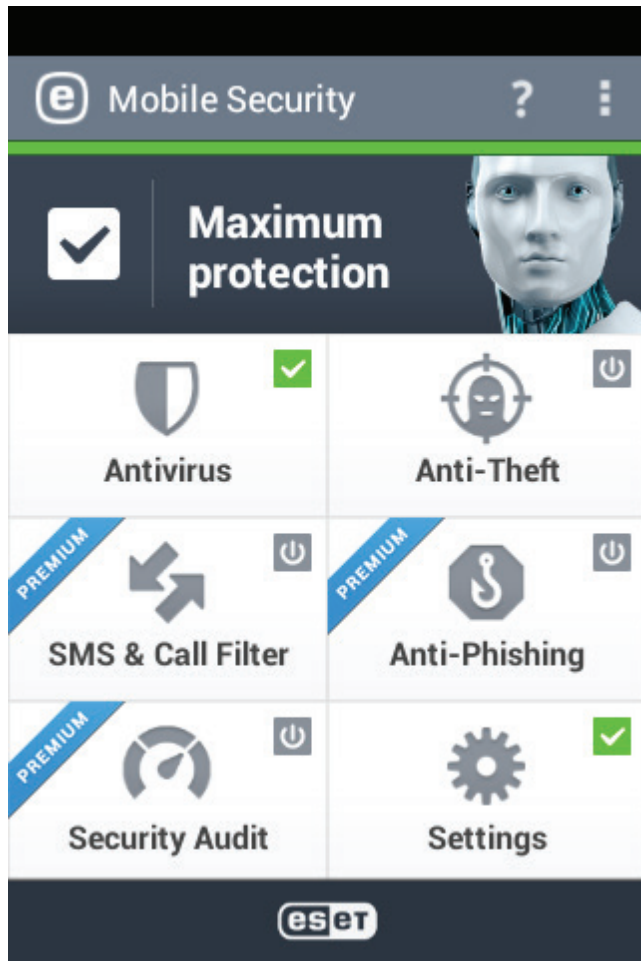
1. Chọn ngôn ngữ hiển thị trong ESET Mobile Security.
2. Chọn đất nước mà bạn đang sinh sống.
3. Nếu bạn muốn giúp ESET cải thiện sản phẩm bằng việc gửi các dữ liệu liên quan đến ứng dụng, chọn appropriate option.
4. Chọn **Accept**. Khi ấy, bạn đồng ý với điều khoản sử dụng của Eset.
5. Chọn nếu bạn muốn tham gia vào ESET Live Grid. Để biết thêm về ESET Live Grid, Xem [this section](#) ^[8].
6. Chọn **Next**.
7. Chọn nếu bạn muốn ESET Mobile Security phát hiện những ứng dụng không mong muốn. Chi tiết về các ứng dụng này có thể tìm thấy tại [this section](#) ^[8].
8. Chọn **Next**.
9. Chọn **Finish**.

2.5 Gỡ bỏ cài đặt

Muốn gỡ bỏ cài đặt ESET Mobile Security. Sử dụng hướng dẫn gỡ bỏ có sẵn trong các lựa chọn trên màn hình chính:**Settings > Uninstall**. Khi yêu cầu gỡ bỏ, bạn phải điền mật khẩu bảo vệ



3. Giấy phép



Sau khi cài đặt thành công, ESET Mobile Security phải được kích hoạt. Để mở khu vực **Giấy Phép**. Chọn biểu tượng  trên màn hình chính của ESET Mobile Security (hoặc nhấn nút **MENU**) và chọn **Giấy Phép**.

Phương pháp kích hoạt sẽ khác nhau tùy thuộc vào bạn tải ESET Mobile Security từ website ESET, Amazon hay Google Play

- **Mua Giấy phép** – Chọn tính năng này nếu bạn chưa có giấy phép và có ý định mua. Bạn sẽ được chuyển hướng đến website của nhà phân phối vùng của ESET.

Mỗi giấy phép đều có thời hạn sử dụng. Sau khi hết hạn, Bạn sẽ được yêu cầu tái kích hoạt (chương trình sẽ tự động nhắc nhở bạn trước khi hết hạn).

LƯU Ý: Trong quá trình kích hoạt, thiết bị phải có kết nối Internet. Một lượng dữ liệu nhỏ sẽ được tải về.

- **Bản dùng thử** - Chọn tính năng dùng thử nếu bạn chưa có giấy phép và thích trải nghiệm ESET Mobile Security trước khi mua. Điền **địa chỉ email** để kích hoạt ESET Mobile Security trong thời gian dùng thử. Bạn sẽ nhận được email xác nhận sau khi kích hoạt sản phẩm thành công. Chỉ có thể kích hoạt giấy phép dùng thử 1 lần 1 thiết bị.
- **Kích hoạt ứng dụng sử dụng Tên đăng nhập và Mật khẩu** - Nếu bạn mua sản phẩm từ nhà phân phối ESET, bạn sẽ nhận được Tên đăng nhập và Mật khẩu. Điền **Tên đăng nhập** và **Mật khẩu** khi được yêu cầu.
- **Kích hoạt ứng dụng sử dụng Mã kích hoạt** – Nếu bạn nhận chương trình với một thiết bị mới (hoặc sản phẩm được cài đặt sẵn), bạn sẽ nhận được **Mã kích hoạt** khi mua. Điền thông tin đó và **địa chỉ email** vào khi được yêu cầu. Thông tin xác nhận (Tên người dùng và Mật khẩu) sẽ tự động thay thế cho mã kích hoạt và được gửi chi tiết về email đăng ký của bạn.

4. Diệt virus

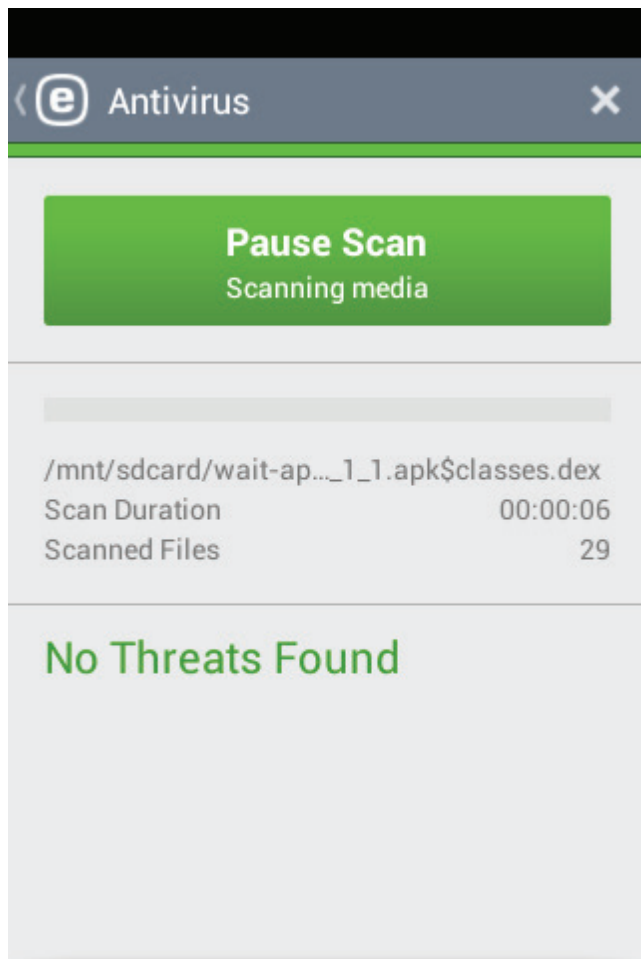
Các trình chống virus sẽ bảo vệ bạn chống lại các mã độc bằng cách khoá tất cả các mối nguy hiểm bằng cách dọn dẹp sạch hoặc cách ly chúng.

Quét thiết bị

Quét thiết bị được dùng để kiểm tra sự xâm nhập cho thiết bị.

Một số loại tập tin quan trọng sẽ được xác định để quét theo mặc định. Quét đầy đủ sẽ kiểm tra bộ nhớ, tiến trình, các thư viện động, cũng như một phần của các bộ nhớ trong hoặc bộ nhớ ngoài. Bảng tóm tắt tiến trình quét sẽ được lưu trong tập tin ở khu vực **Scan Logs**.

Nếu bạn muốn bỏ qua tiến trình quét, chọn biểu tượng .



Cấp độ quét

Có 3 cấp độ quét cho bạn chọn:

- **Nhanh** – Khi chọn chế độ này, ESET Mobile Security chỉ quét ứng dụng cài đặt, tập tin DEX (các tập tin thực thi cho hệ điều hành Android), tập tin SO (thư viện) và tập tin ZIP, tối đa 3 lần nén lồng nhau
- **Thông minh** – Chỉ quét nội dung thẻ SD và các tập tin bằng chế độ quét nhanh
- **Sâu** - quét toàn bộ mọi loại tập tin, phần mở rộng bất kể cả bộ nhớ và thẻ SD

Quét tự động

Bên cạnh chế độ quét theo nhu cầu, ESET Mobile Security cũng cung cấp chế độ quét tự động. Tìm hiểu cách sử dụng On-Charger Scan và Scheduled Scan, [đọc phần này trang 7](#)

Cách ly

Mục đích chính nhằm đảm bảo an toàn khi chứa các tập tin đã bị lây nhiễm. Tìm hiểu thêm, xem [Cách ly trang 8](#)

Bỏ qua mối nguy hại

Tìm hiểu thêm về tính năng này, [xem trang 8](#)

Ghi thông tin quét

Khu vực **Scan Logs** chứa dữ liệu chi tiết về quá trình quét đã hoàn tất trong 1 tập tin. Chi tiết có thể tìm thấy trong [trang 8](#)

Cập thông cơ sở dữ liệu về thông tin các mối nguy hiểm

Mặc định, ESET Mobile Security sẽ tự động nhằm đảm bảo chương trình được cập nhật thường xuyên. Để chạy nâng cấp thủ công, chọn **Update Threat Database**

LƯU Ý: Nhằm tránh việc sử dụng băng thông không cần thiết, chỉ nâng cấp khi cần thiết hoặc khi có mối nguy hại mới được cập nhật. Trong khi nâng cấp miễn phí mối nguy hại, bạn có thể bị tính phí bởi nhà mạng cho việc truyền dữ liệu.

Thông tin chi tiết của Antivirus Advanced Setting có thể được tìm thấy trong phần **Advanced Setting** [trang 8](#)

4.1 Quét tự động

Mức độ quét

Có 3 mức độ quét khác nhau để lựa chọn. Thiết lập này sẽ được áp dụng cho Quét khi sạc và Quét theo lịch:

- **Nhanh** – Khi chọn chế độ này, ESET Mobile Security chỉ quét ứng dụng cài đặt, tập tin DEX (các tập tin thực thi cho hệ điều hành Android), tập tin SO (thư viện) và tập tin ZIP, tối đa 3 lần nén lồng nhau
- **Thông minh** – Chỉ quét nội dung thẻ SD và các tập tin bằng chế độ quét nhanh
- **Sâu** - quét toàn bộ mọi loại tập tin, phần mở rộng bất kể cả bộ nhớ và thẻ SD

Quét khi sạc

Khi chọn tính năng này, tự động quét thiết bị ở trạng thái rảnh khi pin đầy hay được cắm sạc

Quét theo lịch

Quét theo lịch cho phép bạn quét thiết bị một cách tự động vào thời gian định sẵn. Để tạo lịch quét, chọn nút  bên cạnh Scheduled Scan và lên lịch chi tiết. Mặc định, tất cả các ngày trong tuần được chọn

4.2 Cách ly

Các tệp tin cần được cách ly nếu chúng không thể được làm sạch, nếu không an toàn hoặc nếu chúng bị phát hiện sai bởi ESET Mobile Security.

Các tệp được lưu trữ trong khu vực Cách ly có thể được xem trong nhật ký hiển thị tên và vị trí ban đầu của tệp bị nhiễm cùng với ngày và giờ mà tệp đó đã bị cách ly.

Nếu bạn muốn khôi phục lại một tệp tin bị kiểm dịch đến vị trí ban đầu của nó, chọn tệp tin và chọn biểu tượng . Chúng tôi không khuyến khích bạn thường xuyên khôi phục các tệp được kiểm dịch.

Để loại bỏ vĩnh viễn tệp tin bị cách ly từ điện thoại, chọn tệp tin và chọn biểu tượng .

LƯU Ý: Nếu bạn cách ly một ứng dụng đáng ngờ nhưng sau đó chọn cài đặt nó, ứng dụng sẽ tự động được xóa khỏi vùng cách ly.

4.3 Bỏ qua mối nguy hiểm

Trong quá trình quét, bạn có thể thêm một mối đe dọa mới vào danh sách sạch. Mối đe dọa đó sẽ bị bỏ qua cho những lần quét sau này.

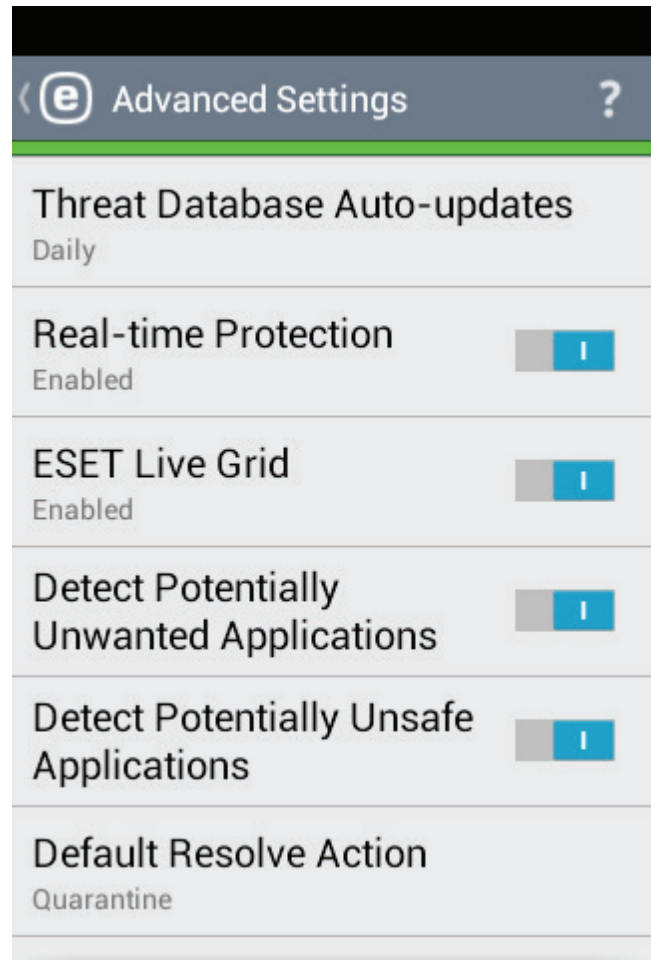
4.4 Thông tin quét

Thông tin quét được tạo ra sau mỗi lần quét theo lịch hoặc thủ công của thiết bị.

Thông tin quét chứa:

- Ngày và giờ của sự kiện
- Thời gian quét
- Số tệp tin được quét
- Kết quả quét hoặc lỗi phát sinh trong suốt quá trình quét

4.5 Cấu hình nâng cao



Tự động cập nhật dữ liệu

Lựa chọn này cho phép bạn thiết lập khoảng thời gian giữa những lần tự động cập nhật dữ liệu tải về. Việc đó giúp nó chỉ cập nhật khi cần thiết. Chúng tôi khuyến khích bạn chọn chế độ mặc định (hàng ngày).

Bảo vệ theo thời gian thực

Lựa chọn này cho phép bạn mở/tắt tính năng bảo vệ theo thời gian thật. Nó sẽ bắt đầu quét tự động khi hệ thống khởi động và quét các tệp tin bạn tương tác. Tự động quét các thư mục tải về, các tệp tin cài đặt .apk và tất cả tệp tin trên thẻ nhớ khi được kết nối.

ESET Live Grid

Được xây dựng dựa trên ThreatSense.Net Hệ thống cảnh báo sớm tiên tiến, **ESET Live Grid** được thiết kế để cung cấp thêm nhiều lớp bảo mật cho thiết bị. Liên tục giám sát các chương trình và tiến trình chạy trong hệ thống, dựa trên các thông tin được thu thập của hàng triệu người dùng trên khắp thế giới. Thêm vào đó, Tiến trình quét rất nhanh và chính xác vì có hệ thống dữ liệu được cập nhật liên tục của ESET Live Grid. Nó giúp chúng tôi bảo vệ kịp thời đến mọi người dùng ESET. Chúng tôi khuyến khích bạn kích hoạt tính năng này. Cảm ơn vì đã hỗ trợ.

Phát hiện các ứng dụng không mong muốn

Ứng dụng không mong muốn là một chương trình có chứa phần mềm quảng cáo, cài đặt thanh công cụ, theo dõi kết quả tìm kiếm hoặc có các mục tiêu khác không rõ ràng. Một số tình huống mà bạn có thể cảm thấy rằng lợi ích của các ứng dụng không mong muốn lớn hơn những rủi ro. Vì lý do này, ESET gán cho các ứng dụng loại rủi ro thấp hơn so với các loại phần mềm độc hại.

Phát hiện các ứng dụng không an toàn

Có nhiều ứng dụng hợp pháp có chức năng đơn giản hóa việc quản lý các thiết bị nối mạng. Tuy nhiên, trong 1 số trường hợp, chúng có thể bị lạm dụng vì các mục đích độc hại. Tùy chọn **Phát hiện các ứng dụng không an toàn** cho phép bạn khám phá những mối đe dọa như vậy. "Các ứng dụng tiềm ẩn không an toàn" là phân loại được sử dụng cho phần mềm thương mại, hợp pháp. Việc phân loại này bao gồm các chương trình như công cụ truy cập từ xa, ứng dụng crack mật khẩu và keylogger.

Cơ chế giải quyết mặc định

Lựa chọn này xác định những hành động sẽ được thực thi sau khi quá trình quét hoàn thành và các mối đe dọa được tìm thấy. Nếu bạn chọn **Remove**, các tập tin lây nhiễm sẽ bị xóa. Nếu bạn chọn **Cách ly**, các tập tin lây nhiễm sẽ bị cách ly .

Máy chủ cập nhật

Trong tùy chọn này, bạn có thể chuyển sang cập nhật cơ sở dữ liệu các mối nguy hại từ **máy chủ Pre-release**. Bản cập nhật trước khi phát hành đã trải qua các thử nghiệm nội bộ cẩn thận và sẽ sớm được công bố rộng rãi cho công chúng. Bạn có thể hưởng lợi từ việc cho phép cập nhật trước khi phát hành bằng cách tiếp cận vào các phương pháp phát hiện mới nhất và các bản sửa lỗi. Tuy nhiên, bản cập nhật trước khi phát hành có thể không hoàn toàn ổn định. Danh sách mô-đun hiện tại có thể được tìm thấy trong phần About: chọn

Menu, biểu tượng  trong màn hình chính ESET Mobile Security (hoặc nhấn nút MENU trên thiết bị) và chọn **About > Application version**. Khuyến khích người dùng chọn mặc định là **Release server**

5. Chống trộm

Tính năng chống trộm bảo vệ thiết bị di động khỏi bị truy cập trái phép.

Nếu bạn mất điện thoại hoặc ai đó ăn cắp nó và bị thay thế thẻ SIM khác, thiết bị sẽ tự động bị khóa bởi ESET Mobile Security và một tin nhắn cảnh báo sẽ được gửi đến (các) số điện thoại do người dùng định sẵn. Thông báo này sẽ bao gồm số điện thoại của thẻ SIM hiện đang được chèn vào, số IMSI (Số nhận dạng thuê bao di động quốc tế) và số IMEI (Số điện thoại di động) của điện thoại. Người dùng trái phép sẽ không nhận thức được rằng tin nhắn này đã được gửi bởi vì nó sẽ tự động bị xóa thiết bị của bạn. Bạn cũng có thể biết tọa độ GPS của thiết bị di động bị mất hoặc xóa tất cả dữ liệu được lưu trữ trên thiết bị từ xa.

LƯU Ý: một vài tính năng chống trộm (tin nhắn bảo vệ, bạn bè tin cậy hay ra lệnh bằng SMS) sẽ không sử dụng được trên các máy tính bảng không hỗ trợ gửi tin nhắn.

Phiên bản 3 của ESET Mobile Security được tích hợp tính năng chống trộm của ESET thông qua my.eset.com. Điều này cho phép bạn giám sát hoạt động của thiết bị từ cổng trực tuyến ESET, khóa thiết bị, gửi tin nhắn tùy chỉnh tới trình tìm thiết bị, kích hoạt tiếng còi lớn hoặc xóa dữ liệu thiết bị từ xa.

Để bắt đầu sử dụng tính năng chống trộm, bấm **Anti-Theft** trong màn hình chính. Một giao diện đơn giản sẽ hướng dẫn bạn tạo mật khẩu bảo mật, kích hoạt tính năng chống gỡ bỏ, định nghĩa SIM tin cậy, danh sách những người bạn tin cậy, nhập chi tiết liên lạc của bạn và kích hoạt câu lệnh từ SMS. Khi các bước này hoàn tất, bạn có thể liên kết thiết bị của mình với tài khoản my.eset.com.

5.1 my.eset.com

Nếu bạn đã có tài khoản my.eset.com, chọn **Already have an account?** điền địa chỉ mail và mật khẩu để đăng nhập.

Nếu bạn không có tài khoản my.eset.com, nhấn **Register** và điền vào mẫu đăng ký. Kiểm tra hộp thư đến của bạn để xác nhận email và nhấp vào liên kết để kích hoạt tài khoản của bạn. Bây giờ bạn có thể tận hưởng các tính năng bảo mật chống trộm được quản lý từ my.eset.com.

Chi tiết về sử dụng tính năng chống trộm tại my.eset.com, tham khảo trợ giúp trực tuyến – chọn **Help** trên góc phải phía trên của màn hình.

5.2 Tối ưu hoá

Tối ưu hóa Chống trộm ESET là một đánh giá kỹ thuật có thể đo lường được về trạng thái bảo mật của thiết bị của bạn. Bảo vệ chống trộm của ESET sẽ kiểm tra hệ thống của bạn các vấn đề sau:

- Tắt dịch vụ định vị
- Không sử dụng vệ tinh GPS
- Mã khóa màn hình không an toàn
- Chưa mở dữ liệu Mobile
- Không có dịch vụ Google Play

Khi có vấn đề bảo mật, bạn có thể chọn Change Setting để thay đổi

điều hướng tới màn hình nơi bạn có thể giải quyết vấn đề cụ thể đó. Nếu bạn không muốn ESET Mobile Security báo cáo sự cố này, hãy nhấn Ignore this issue

5.3 Bảo vệ Sim

Phần bảo vệ SIM hiển thị danh sách các thẻ SIM đáng tin cậy sẽ được chấp nhận bởi ESET Mobile Security. Nếu bạn chèn một thẻ SIM không được định nghĩa trong danh sách này, màn hình sẽ bị khóa và cảnh báo tin nhắn SMS sẽ được gửi đến bạn bè tin cậy của bạn.

Để thêm 1 thẻ SIM mới, chọn biểu tượng . Tìm hiểu thêm, xem [trang 101](#).

Để xóa 1 thẻ SIM khỏi danh sách, chọn và giữ SIM, và chọn biểu tượng .

LƯU Ý: Tính năng SIM Guard không hỗ trợ cho thiết bị CDMA và WCDMA

5.3.1 Thêm 1 sim tin cậy

Nhập Tên cho thẻ SIM (ví dụ: Nhà, Cơ quan) và IMSI (Số nhận dạng thuê bao di động quốc tế). IMSI thường được trình bày như một số dài 15 chữ số được in trên thẻ SIM của bạn. Trong một số trường hợp, nó có thể ngắn hơn.

5.4 Bạn bè tin cậy

Trong danh sách Bạn bè tin cậy, bạn có thể thêm hoặc xóa số điện thoại sẽ nhận được một tin nhắn SMS thông báo sau khi thẻ SIM không đáng tin cậy được gắn vào thiết bị của bạn. Để thêm một người bạn đáng tin cậy mới, bấm Thêm từ Add from Contacts và chọn một số liên lạc từ danh sách liên lạc của bạn.

Nếu người đó không nằm trong danh bạ, chọn biểu tượng . Tìm hiểu thêm, xem [trang 101](#).

Để xóa số khỏi danh bạ, chạm và giữ số, kéo vào biểu tượng .

LƯU Ý: Nếu bạn ở nước ngoài, tất cả các số điện thoại được nhập trong danh sách phải bao gồm mã quay số quốc tế, sau đó là số thực (ví dụ: +1610100100).

5.4.1 Thêm bạn tin cậy

Nhập tên của bạn bè và số điện thoại của họ. Nếu số liên lạc chứa nhiều số điện thoại, tin nhắn SMS sẽ được gửi đến tất cả các số liên quan. Nếu bạn muốn cho phép người bạn này đặt lại mật khẩu của bạn trong trường hợp bạn quên nó, hãy chọn tùy chọn **Allow remote reset of the password**.

5.5 Tập lệnh tin nhắn

Các lệnh sms từ xa (khóa, cài báo động, tìm và xóa) sẽ chỉ hoạt động nếu lệnh **Vấn bản SMS** được kích hoạt.

Nếu bạn mất điện thoại và muốn khóa điện thoại, hãy gửi một tin nhắn SMS từ khóa từ bất kỳ thiết bị di động nào tới số điện thoại của bạn dưới dạng sau:

eset lock password

Thay *password* bằng mật khẩu bảo mật của bạn. Khi thiết bị của bạn bị khóa, người dùng trái phép sẽ được yêu cầu nhập mật khẩu của bạn để mở khóa.

Để khóa thiết bị của bạn và kích hoạt còi báo động, hãy gửi một

tin nhắn SMS đến số điện thoại của bạn theo cú pháp sau:

eset siren password.

Còi sẽ hú kể cả khi thiết bị đang bị tắt âm thanh.

Nếu bạn muốn yêu cầu tọa độ GPS của thiết bị di động của bạn, hãy gửi tin nhắn văn bản đến số di động của bạn hoặc số điện thoại di động của người dùng trái phép (nếu thẻ SIM đã được thay thế) dưới dạng sau:

eset find password

Bạn sẽ nhận được một tin nhắn văn bản với GPS tọa độ của thiết bị bị mất của bạn bao gồm một liên kết đến vị trí đó trên bản đồ của Google.

Nếu bạn muốn xóa tất cả dữ liệu được lưu trữ trên thiết bị của bạn và tất cả các bộ nhớ gắn ngoài hiện đang được gắn, gửi tin nhắn SMS đến điện thoại của bạn trong theo cú pháp sau:

eset wipe password

Tất cả địa chỉ liên hệ, tin nhắn, email, tài khoản, ứng dụng, nội dung thẻ SD, hình ảnh, nhạc và video được lưu trữ trong thư mục mặc định của Android sẽ bị xóa vĩnh viễn khỏi thiết bị của bạn.

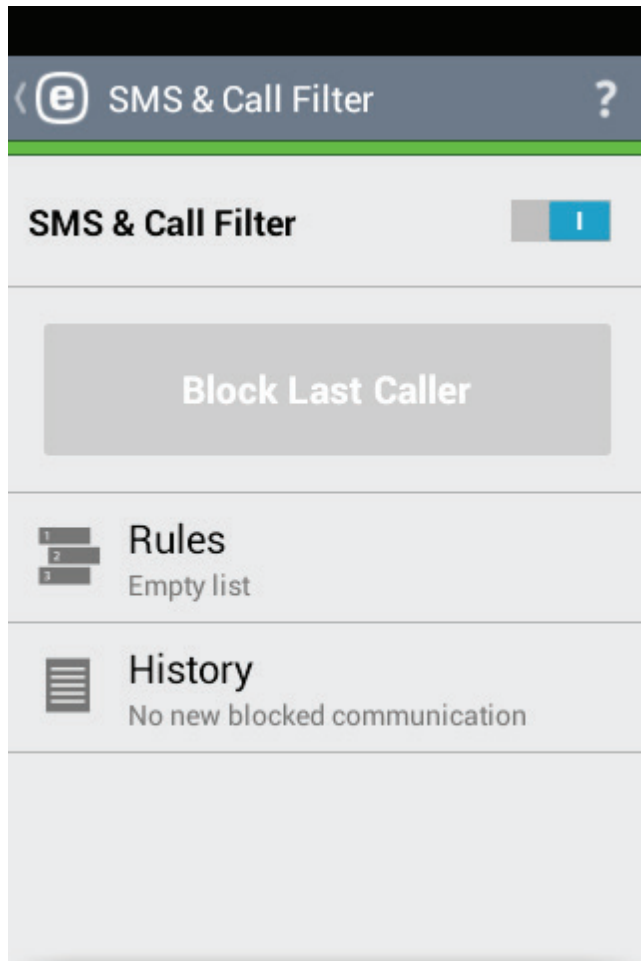
LƯU Ý: Mật khẩu của bạn phân biệt chữ hoa chữ thường. Hãy chắc chắn rằng bạn nhập mật khẩu chính xác như lúc thiết lập.

5.6 Thông tin liên lạc chi tiết

Nếu bạn đánh dấu thiết bị của bạn đã bị thất lạc trên website my.eset.com, Thông tin từ "**Thông tin liên lạc chi tiết**" sẽ được hiển thị trên màn hình thiết bị của bạn để giúp người tìm thấy thiết bị liên lạc với bạn.

Điền vào tên, mô tả thiết bị, số liên hệ dự phòng (ví dụ, số điện thoại nhà hoặc nơi làm việc) hoặc địa chỉ email

6. Tin nhắn & lọc cuộc gọi



SMS & Call Filter chặn các tin nhắn SMS/MMS đến và các cuộc gọi đến/đi dựa trên các quy tắc của bạn

Các tin nhắn không mong muốn thường bao gồm quảng cáo từ các nhà cung cấp dịch vụ điện thoại di động hoặc tin nhắn từ những người dùng nặc danh hoặc không xác định. Cụm từ block message đề cập đến việc di chuyển một thông báo đến phần History một cách tự động. Không có thông báo nào được hiển thị khi một tin nhắn đến bị chặn. Lợi thế của việc này là bạn sẽ không bị làm phiền bởi thông tin không mong muốn, nhưng luôn luôn có thể kiểm tra các bản ghi cho các tin nhắn có thể đã bị chặn do nhầm lẫn.

LƯU Ý: SMS & Call Filter không hoạt động trên máy tính bảng không hỗ trợ tính năng gọi và nhắn tin. SMS & Call Filter không khả dụng cho các thiết bị Android OS 4.4 (KitKat) và sẽ bị tắt trên các thiết bị mà Google Hangouts được đặt làm ứng dụng chính cho SMS.

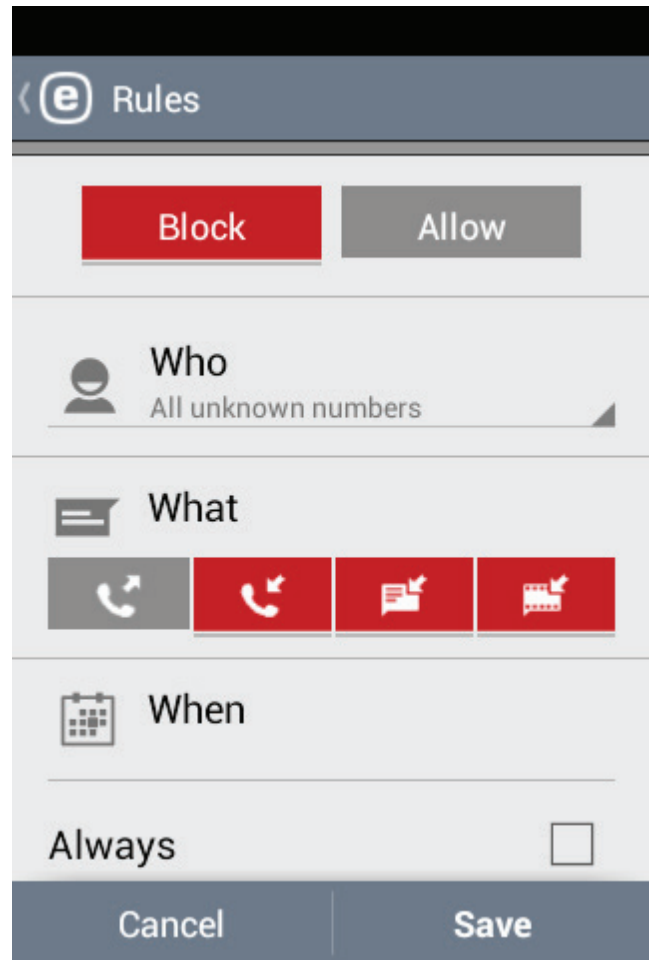
Để chặn các cuộc gọi và tin nhắn từ số điện thoại đã nhận lần cuối, bấm Chặn Người gọi cuối. Điều này sẽ tạo ra một quy tắc mới cho SMS & Call Filter

6.1 Quy tắc

Để thêm quy tắc, chọn biểu tượng . Tìm hiểu thêm về cách tạo quy tắc, tìm trong trang [12](#).

Nếu muốn xoá quy tắc hiện có từ danh sách quy tắc, chạm và giữ, kéo vào biểu tượng .

6.1.1 Thêm quy tắc mới



Chỉ định một nhóm các số điện thoại hoặc một người. **Tất cả số không xác định** sẽ bao gồm số điện thoại không được lưu trong danh sách liên hệ của bạn. Bạn có thể sử dụng tùy chọn này để chặn cuộc gọi điện thoại không mong muốn (ví dụ: "cuộc gọi lạnh") hoặc để ngăn trở không quay số không xác định. Tùy chọn **Tất cả các số đã biết** là tất cả các số điện thoại được lưu trong danh sách liên lạc của bạn. **Số ẩn** sẽ áp dụng cho những người gọi có số điện thoại của họ cố ý giấu qua Calling Line Identification Restriction (CLIR).

Chỉ định cái nào nên chặn hoặc cho phép:

- cuộc gọi đi
- cuộc gọi đến
- tin nhắn đến (SMS) hoặc
- tin nhắn đa phương tiện đến (MMS)

Để áp dụng quy tắc cho một thời gian chỉ định, bỏ chọn **Luôn** ở cuối và chọn ngày và giờ mà bạn muốn áp dụng quy tắc. Theo mặc định, tất cả các ngày trong tuần được chọn. Chức năng này có thể hữu ích nếu bạn không muốn bị quấy rầy vào ban đêm hoặc trong những ngày cuối tuần.

LƯU Ý: Nếu bạn ở nước ngoài, tất cả các số điện thoại được nhập trong danh sách phải bao gồm mã quay số quốc tế, sau đó là số thực (ví dụ: +1610100100).

6.2 Lịch sử

Trong phần Lịch sử, bạn có thể xem các cuộc gọi và tin nhắn bị chặn bởi SMS & Call Filter. Mỗi đăng nhập chứa tên của sự kiện, số điện thoại tương ứng, ngày và thời gian của sự kiện. Bản ghi tin nhắn SMS và MMS cũng chứa nội dung thư.

Nếu bạn muốn sửa đổi một quy tắc liên quan đến số điện thoại hoặc số liên lạc đã bị chặn, hãy chọn mục trong danh sách bằng cách nhấp vào nó và chọn biểu tượng .

Để xoá mục trong danh sách, chọn và nhấp vào biểu tượng . Để xoá nhiều mục, giữ và chạm 1 trong các mục,

Chọn những mục mà bạn muốn xoá và nhấp vào biểu tượng .

7. Chống lừa đảo

Thuật ngữ phishing xác định hoạt động tội phạm sử dụng kỹ thuật xã hội (thôn tính người dùng để có được thông tin bí mật). Phishing thường được sử dụng để truy cập vào dữ liệu nhạy cảm như số tài khoản ngân hàng, số thẻ tín dụng, số PIN hoặc tên người dùng và mật khẩu.

Chúng tôi khuyên bạn nên kích hoạt Anti-Phishing. Tất cả các cuộc tấn công lừa đảo tiềm ẩn đến từ các trang web hoặc tên miền được liệt kê trong cơ sở dữ liệu phần mềm độc hại của ESET sẽ bị chặn và thông báo cảnh báo sẽ được hiển thị thông báo cho bạn về vụ tấn công này.

Anti-Phishing kết hợp với các trình duyệt web phổ biến nhất hiện có trên hệ điều hành Android (ví dụ: Chrome hoặc trình duyệt web Android mặc định).

LƯU Ý: Anti-Phishing đảo sẽ không bảo vệ bạn khi duyệt web ở chế độ riêng (ẩn danh).

7. 1 Lịch sử

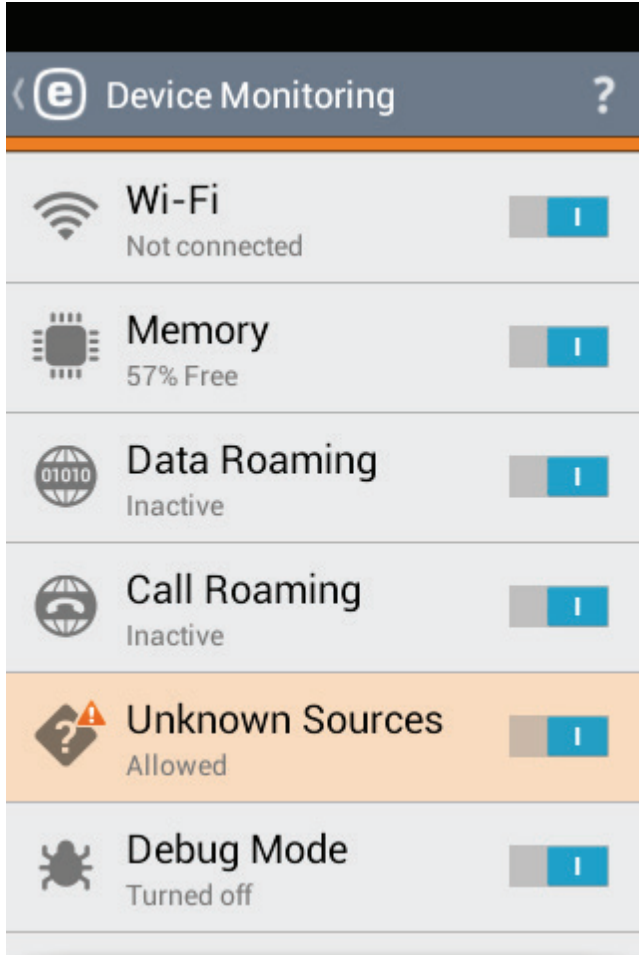
Trong phần lịch sử, bạn có thể xem danh sách tất cả các cuộc tấn công lừa đảo bị chặn bởi ESET Mobile Security.

8. Kiểm tra bảo mật

Kiểm tra an ninh giúp bạn theo dõi và thay đổi cài đặt thiết bị quan trọng và cho phép các ứng dụng đã cài đặt để ngăn ngừa rủi ro bảo mật.

Để bật / tắt kiểm tra bảo mật và các thành phần cụ thể, sử dụng các nút sau: 

8.1 Kiểm tra ứng dụng

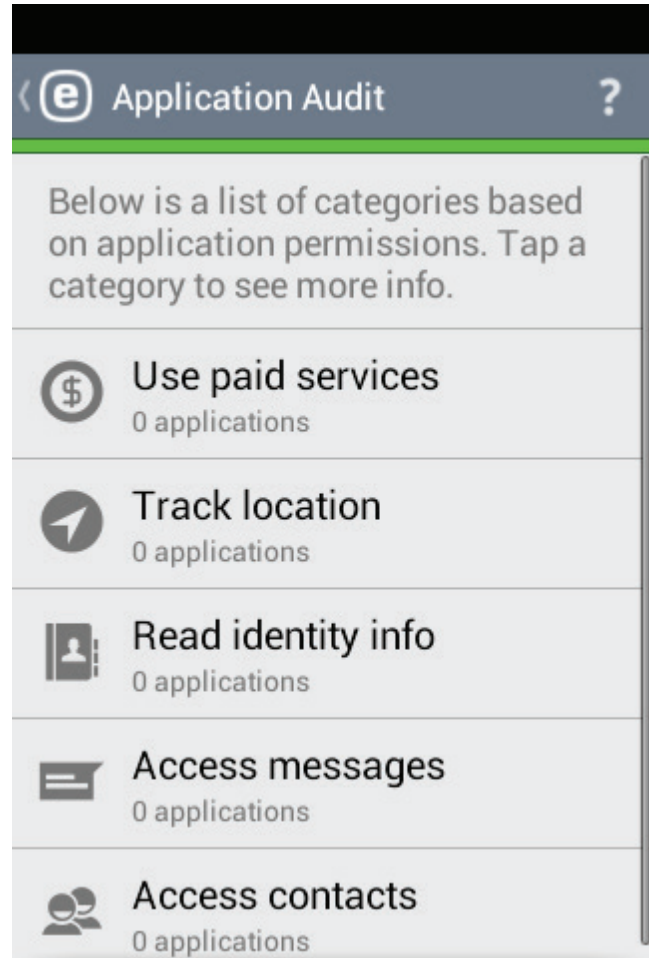


Trong phần Device Monitoring, bạn có thể xác định thành phần thiết bị nào sẽ được giám sát bởi ESET Mobile Security.

Bấm vào mỗi tùy chọn để xem mô tả chi tiết về tùy chọn và tình trạng hiện tại của nó.

Các tùy chọn như **Unknown Sources** và **Debug Mode** có thể được thay đổi bằng cách chạm vào **Change Settings**. Thao tác này sẽ chuyển hướng bạn đến màn hình cài đặt hệ điều hành Android.

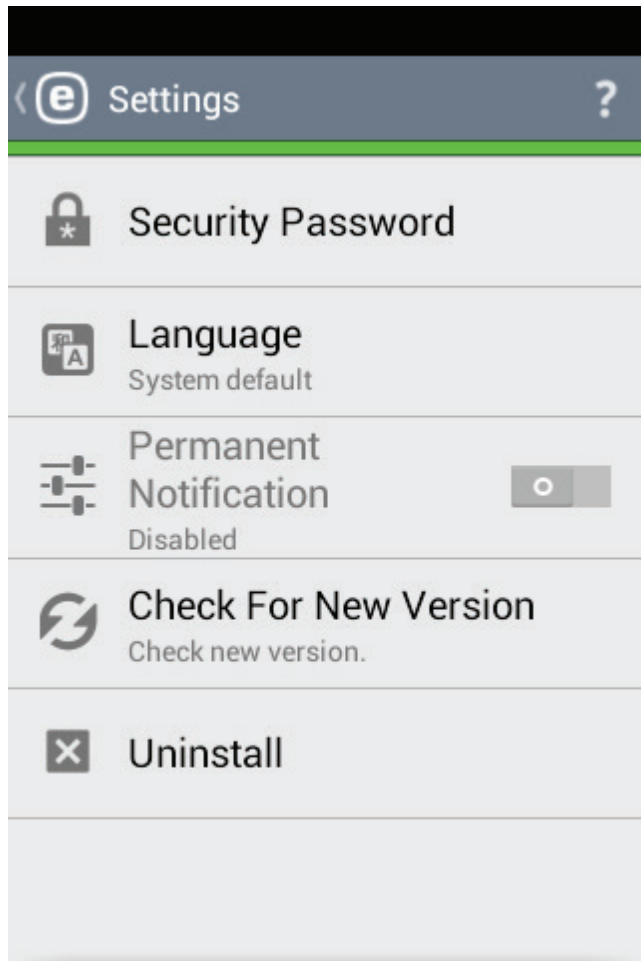
8.2 Giám sát thiết bị



Một số ứng dụng được cài đặt trên thiết bị của bạn có thể có quyền truy cập vào các dịch vụ có tính phí, theo dõi vị trí của bạn hoặc đọc thông tin nhận dạng, địa chỉ liên hệ hoặc tin nhắn văn bản của bạn. ESET Mobile Security cung cấp kiểm soát các ứng dụng này.

Trong phần **Application Audit**, bạn có thể xem danh sách các ứng dụng được sắp xếp theo danh mục. Chạm vào từng danh mục để xem mô tả chi tiết của nó. Các chi tiết quyền của mỗi ứng dụng có thể được truy cập bằng cách chọn ứng dụng đó.

9. Cài đặt



Mật khẩu an toàn

Tùy chọn này cho phép bạn đặt mật khẩu bảo mật mới hoặc thay đổi mật khẩu hiện tại.

Tìm hiểu thêm, xem khu vực [Security Password](#) [16]

Ngôn ngữ

Theo mặc định, ESET Mobile Security được cài đặt bằng ngôn ngữ được đặt trên thiết bị của bạn dưới dạng ngôn ngữ hệ thống (trong cài đặt Ngôn ngữ và bàn phím của Android OS). Để thay đổi ngôn ngữ của giao diện người dùng ứng dụng, bấm **Ngôn ngữ** và chọn ngôn ngữ bạn dùng.

Thông báo vĩnh viễn

ESET Mobile Security hiển thị biểu tượng thông báo  ở góc trên cùng bên trái của màn hình (thanh trạng thái trên Android).

Nếu bạn không muốn biểu tượng này được hiển thị, bỏ chọn **Permanent Notification**

Kiểm tra phiên bản mới

Để bảo vệ tối đa, điều quan trọng là sử dụng phiên bản mới nhất của ESET Mobile Security. Nhấn **Kiểm tra Phiên bản Mới** để xem liệu có phiên bản mới hơn có sẵn để tải xuống hay không.

Gỡ bỏ

Nếu bạn muốn gỡ bỏ cài đặt ESET Mobile Security, sử dụng trình **Uninstall**. Các thư mục ESET Mobile Security và cách ly sẽ được xóa vĩnh viễn.

9.1 Mật khẩu bảo mật.

Mật khẩu an toàn được yêu cầu để mở khóa thiết bị của bạn, truy cập các tính năng được bảo vệ bằng mật khẩu (ví dụ Anti-Theft) và gỡ bỏ cài đặt ESET Mobile Security. Cụm từ lời nhắc (nếu được đặt) hiển thị gợi ý để giúp bạn nhớ mật khẩu của mình.

Nếu bạn quên mật khẩu, bạn có thể gửi tin nhắn từ số điện thoại lưu trong danh sách **Trusted Friends** (trang [10]) đến số điện thoại của mình. Cú pháp tin nhắn như sau: *“eset remote reset”*
Mật khẩu của bạn sẽ được đặt lại và bạn sẽ được yêu cầu đặt lại một mật khẩu mới.

Nếu bạn không có một Người bạn đáng tin cậy đã được định nghĩa sẵn khi khóa thiết bị của mình, bạn có thể gửi yêu cầu đặt lại mật khẩu. Tùy chọn này sẽ hoạt động trên màn hình bị khóa sau 2 lần không thành công để mở khóa thiết bị của bạn. Bạn sẽ nhận được một email có chứa mã mở khóa tại địa chỉ email tài khoản Google của bạn hoặc một địa chỉ email được xác định trong quá trình mua hoặc kích hoạt sản phẩm ESET. Nhập mã mở khóa trên màn hình bị khóa. Khi thiết bị của bạn được mở khóa, hãy xác định mật khẩu bảo mật mới trong **Cài đặt > Mật khẩu**.

Ngoài ra, bạn có thể thay đổi mật khẩu bảo mật của mình tại my.eset.com. Sau khi đăng nhập, chọn thiết bị của bạn, bấm **Cài đặt** và gõ mật khẩu mới.

LƯU Ý: Hãy chọn cẩn thận mật khẩu của bạn. Để tăng tính bảo mật và khó đoán, sử dụng một sự kết hợp của các chữ cái nhỏ, chữ hoa và số.

10. Chăm sóc khách hàng

Các chuyên gia chăm sóc khách hàng của ESET sẵn sàng hỗ trợ hành chính hoặc hỗ trợ kỹ thuật liên quan đến ESET Mobile Security hoặc bất kỳ sản phẩm ESET nào khác.

Để gửi yêu cầu hỗ trợ từ thiết bị, chọn biểu tượng  trong màn hình chính (hoặc nhấn nút **MENU** trên thiết bị) và chọn **Customer Care**. Điền vào tất cả các vùng được yêu cầu.

ESET Mobile Security bao gồm các chức năng ghi lại nhật ký tiên tiến để giúp chẩn đoán các vấn đề kỹ thuật tiềm ẩn. Để cung cấp cho ESET một nhật ký ứng dụng chi tiết, đảm bảo rằng **Application log** được chọn (mặc định). Gửi yêu cầu của bạn bằng cách nhấn vào nút **Submit**. Các chuyên gia chăm sóc khách hàng của ESET sẽ liên hệ với bạn theo địa chỉ email mà bạn cung cấp.