kaspersky

Kaspersky Endpoint Security 10 Service Pack 2 for Windows

Nội dung

Thông tin về Kaspersky Endpoint Security 10 Service Pack 2 for Windows

Phần này mô tả các chức năng, thành phần và bộ phân phối của Kaspersky Endpoint Security, cũng như cung cấp một danh sách các yêu cầu về phần cứng và phần mềm của Kaspersky Endpoint Security.

Có gì mới

Kaspersky Endpoint Security 10 Service Pack 2 for Windows cung cấp các tính năng và cải tiến sau đây:

1. Kiểm soát Khởi động Ứng dụng:
    - Hỗ trợ hệ điều hành máy chủ.
    - Kiểm soát tải về các mô-đun DLL và trình điều khiển.
    - Quản lý danh sách các đối tượng trong tác vụ kiểm kho (mô-đun DLL và tập tin kịch bản)
    - Kiểm soát đối tượng dựa trên một tiêu chí mới - theo thuộc tính của chứng chỉ chữ ký điện tử.
    - Tạo một báo cáo về việc khởi động thử nghiệm ứng dụng bị chặn.
    - Hỗ trợ hai chế độ hoạt động cho Kiểm soát ứng dụng khởi động: "Danh sách Đen" và "Danh sách Trắng".
    - Sử dụng hash SHA256 để kiểm soát và kiểm kho các đối tượng.
    - Kiểm soát việc chạy các kịch bản từ trình biên dịch PowerShell.
    - Sử dụng ổ lưu trữ chứng chỉ hệ thống được tin tưởng.
2. Quản lý Microsoft BitLocker cho phép mã hóa các ổ cứng với sự trợ giúp của công nghệ BitLocker từ Microsoft:
    - Quản lý mã hóa từ xa.
    - Giám sát các thiết bị được mã hóa.
    - Tạo các báo cáo mã hóa thiết bị.
    - Khôi phục truy cập đến các thiết bị được mã hóa.
3. Kaspersky Disk Encryption:
    - Hỗ trợ nhập chứng chỉ trong chế độ tiền khởi động của Authentication Agent sử dụng một bàn phím ảo.
    - Hỗ trợ chế độ mã hóa để chỉ mã hóa dung lượng được sử dụng trên một thiết bị.
    - Hỗ trợ mã hóa trên máy tính bảng (MS Surface phiên bản 3 và 4).
4. Kiểm soát Đặc quyền Ứng dụng:

- Kiểm soát truy cập của ứng dụng đến các thiết bị ghi âm và ghi video.

5. Kiểm soát web:
   - Cấu hình các quy tắc truy cập tài nguyên web cho các hạng mục tài nguyên web khác.
6. Kiểm soát Thiết bị:
   - Ghi lại các sự kiện liên quan đến việc xóa và lưu tập tin trên các thiết bị USB.
   - Tạo một danh sách các mạng Wi-Fi được tin tưởng dựa trên các cấu hình sau: tên, kiểu mã hóa và kiểu xác thực.
   - Quản lý quyền truy cập của người dùng cho các tác vụ đọc và ghi trên các đĩa CD/DVD.
7. Chống virus cho thư điện tử:
   - Khả năng xóa và đổi tên các tập tin thuộc loại cụ thể trong các tập nén để được quét bởi Chống virus cho thư điện tử.
8. Kaspersky Security Network:
   - Cho thấy KSN là một lý do cho quyết định liên quan đến phương thức xử lý đối tượng trong các báo cáo của Kaspersky Endpoint Security và Kaspersky Security Center.
   - Gửi một truy vấn đến KSN liên quan đến danh tiếng của một tập tin được chọn.
   - Hiển thị trạng thái khả dụng của máy chủ KSN cho các máy khách có cài đặt Kaspersky Endpoint Security.

Gói phân phối

Bộ phân phối Kaspersky Endpoint Security chứa các tập tin sau:

- Các tập tin cần thiết cho việc cài đặt ứng dụng sử dụng bất kỳ phương thức khả dụng nào:
- Các tập tin trong gói cập nhật được sử dụng trong quá trình cài đặt ứng dụng
- Tập tin klcfginst.msi để cài đặt tiện ích quản trị Kaspersky Endpoint Security thông qua Kaspersky Security Center.
- Tập tin ksn_<language ID>.txt mà trong đó bạn có thể xem các điều khoản tham gia vào Kaspersky Security Network.
- Tập tin license.txt mà trong đó bạn có thể xem Thỏa thuận giấy phép người dùng cuối.
- Tập tin incompatible.txt chứa một danh sách các phần mềm không tương thích.
- Tập tin installer.ini chứa cấu hình nội bộ của gói phân phối.

> Bạn không nên thay đổi các giá trị của những cấu hình này. Nếu bạn muốn thay đổi tùy chọn cài đặt, hãy sử dụng tập tin setup.ini.

Bạn phải giải nén gói phân phối để truy cập các tập tin.

Tổ chức tính năng bảo vệ máy tính

Kaspersky Endpoint Security cung cấp bảo vệ máy tính toàn diện chống lại nhiều mối đe dọa, tấn công mạng và tấn công lừa đảo khác nhau.

Mỗi loại mối đe dọa đều được xử lý bởi một thành phần chuyên dụng. Các thành phần có thể được kích hoạt hoặc vô hiệu hóa độc lập với nhau, và các thiết lập của họ có thể được cấu hình.

Ngoài tính năng bảo vệ thời gian thực được cung cấp bởi các thành phần ứng dụng, chúng tôi khuyên bạn nên thường xuyên *quét* máy tính để phát hiện virus và các mối đe dọa khác. Điều này giúp loại trừ nguy cơ phân tán phần mềm độc hại không được phát hiện bởi các thành phần bảo vệ do cấu hình bảo mật thấp hoặc vì các lý do khác.

Để giữ cho Kaspersky Endpoint Security được cập nhật, bạn cần phải *cập nhật* cơ sở dữ liệu và các mô-đun được sử dụng bởi ứng dụng. Ứng dụng sẽ tự động được cập nhật theo mặc định, nhưng nếu cần thiết, bạn có thể cập nhật cơ sở dữ liệu và các mô-đun ứng dụng một cách thủ công.

Các thành phần ứng dụng sau đây là các thành phần kiểm soát:

- **Kiểm soát ứng dụng khởi động**. Thành phần này theo dõi các nỗ lực của người dùng để khởi chạy ứng dụng và điều tiết việc khởi chạy các ứng dụng.
- **Kiểm soát Đặc quyền Ứng dụng**. Thành phần này đăng ký hành động của các ứng dụng trong hệ điều hành và điều tiết hoạt động của ứng dụng tùy thuộc vào nhóm tin tưởng của một ứng dụng cụ thể. Một tập hợp các quy tắc được quy định cho từng nhóm ứng dụng. Các quy tắc này điều tiết việc truy cập của ứng dụng đến dữ liệu người dùng cũng như đến các tài nguyên của hệ điều hành. Các dữ liệu đó bao gồm tập tin người dùng (thư mục My Documents, cookies, thông tin hoạt động người dùng) và các tập tin, thư mục và khóa registry chứa cấu hình và thông tin quan trọng từ những ứng dụng được sử dụng thường xuyên nhất.
- **Giám sát Lỗ hổng Bảo mật**. Thành phần Giám sát Lỗ hổng bảo mật chạy tác vụ quét lỗ hổng bảo mật trong thời gian thực cho các ứng dụng được khởi chạy, hoặc đang chạy trên máy tính của người dùng.
- **Kiểm soát Thiết bị**. Thành phần này cho phép bạn đặt các hạn chế linh hoạt cho việc truy cập đến các thiết bị lưu trữ dữ liệu (ví dụ như ổ đĩa di động, ổ đĩa di động, ổ băng, và đĩa CD/DVD), các thiết bị truyền tải dữ liệu (ví dụ như modem), các thiết bị chuyển đổi thông tin thành bản sao cứng (ví dụ như máy in), hoặc các giao diện kết nối thiết bị đến các máy tính (ví dụ như USB, Bluetooth và Hồng ngoại).
- **Kiểm soát web**. Thành phần này cho phép bạn đặt các hạn chế linh hoạt cho việc truy cập đến các tài nguyên web cho các nhóm người dùng khác nhau.

Hoạt động của các thành phần kiểm soát được dựa trên các quy tắc sau:

- Kiểm soát ứng dụng khởi động sử dụng các quy tắc Kiểm soát ứng dụng khởi động.
- Kiểm soát Đặc quyền Ứng dụng sử dụng các quy tắc Kiểm soát Ứng dụng.
- Kiểm soát Thiết bị sử dụng quy tắc truy cập thiết bị và quy tắc truy cập bus kết nối.
- Kiểm soát web sử dụng các quy tắc truy cập tài nguyên web.

Các thành phần ứng dụng sau đây là các thành phần bảo vệ:

- **Chống virus cho tập tin**. Thành phần này sẽ bảo vệ hệ thống tập tin của máy tính khỏi nhiễm virus. Chống virus cho tập tin sẽ khởi động cùng với Kaspersky Endpoint Security, liên tục hoạt động trong bộ nhớ máy tính và quét tất cả các tập tin được mở ra, lưu lại hoặc khởi động trên máy tính và trên tất cả các ổ đĩa được kết nối. Chống virus cho tập tin sẽ theo dõi tất cả các nỗ lực truy cập vào một tập tin và quét các tập tin để phát hiện virus và các mối đe dọa khác.

- **Giám sát Hệ thống**. Thành phần này lưu hồ sơ về hoạt động của ứng dụng trên máy tính và cung cấp thông tin này đến các thành phần khác để đảm bảo bảo vệ máy tính một cách hiệu quả hơn.

- **Chống virus cho thư điện tử**. Thành phần này sẽ quét các email đến và đi để phát hiện virus và các mối đe dọa khác.

- **Chống virus cho web**. Thành phần này sẽ quét lưu lượng đến máy tính của người dùng qua các giao thức HTTP và FTP, và kiểm tra liệu các URL có phải là các địa chỉ web độc hại hoặc lừa đảo hay không.

- **Chống virus cho tin nhắn**. Thành phần này sẽ quét lưu lượng đến máy tính thông qua các giao thức của ứng dụng nhắn tin nhanh. Thành phần này cho phép bạn sử dụng rất nhiều ứng dụng nhắn tin nhanh một cách bảo mật.

- **Tường lửa**. Thành phần này bảo vệ dữ liệu được lưu trữ trên máy tính của bạn và chặn hầu hết các mối đe dọa tiềm năng đến hệ điều hành trong khi máy tính đang được kết nối đến Internet hoặc đến một mạng máy tính cục bộ. Thành phần này sẽ lọc mọi hoạt động mạng theo hai dạng quy tắc: quy tắc mạng cho ứng dụng và quy tắc gói tin mạng.

- **Giám sát mạng**. Thành phần này cho phép bạn xem hoạt động mạng của một máy tính trong thời gian thực.

- **Ngăn chặn tấn công mạng**. Thành phần này sẽ kiểm tra lưu lượng mạng vào để phát hiện các hoạt động tương tự với các cuộc tấn công mạng. Khi phát hiện một nỗ lực tấn công mạng nhắm vào máy tính của bạn, Kaspersky Endpoint Security sẽ chặn hoạt động mạng từ máy tính tấn công.

Các tác vụ sau được cung cấp trong Kaspersky Endpoint Security:

- **Quét Toàn bộ**. Kaspersky Endpoint Security sẽ quét hệ điều hành, bao gồm RAM, các đối tượng được nạp khi khởi động, ổ lưu trữ sao lưu của hệ điều hành, cùng tất cả ổ cứng và ổ đĩa di động.

- **Quét Tùy chỉnh**. Kaspersky Endpoint Security sẽ quét các đối tượng được chọn bởi người dùng.

- **Quét khu vực quan trọng**. Kaspersky Endpoint Security sẽ quét các đối tượng được nạp lúc khởi động hệ điều hành, RAM, và các đối tượng được nhắm đến bởi rootkit.

- **Cập nhật**. Kaspersky Endpoint Security sẽ tải về các bản cập nhật cho cơ sở dữ liệu và mô-đun ứng dụng. Việc cập nhật giúp máy tính luôn được bảo vệ chống lại các virus mới nhất cùng các mối đe dọa khác.

- **Quét lỗ hổng bảo mật**. Kaspersky Endpoint Security sẽ quét hệ điều hành và phần mềm được cài đặt để phát hiện lỗ hổng bảo mật. Việc quét đảm bảo phát hiện và xử lý kịp thời các vấn đề tiềm năng mà kẻ xâm nhập có thể khai thác.

Chức năng mã hóa tập tin cho phép bạn mã hóa các tập tin và thư mục được lưu trữ trên ổ đĩa cục bộ của máy tính. Chức năng mã hóa ổ đĩa cho phép mã hóa các ổ cứng và ổ đĩa di động.

Quản trị từ xa thông qua Kaspersky Security Center

Kaspersky Security Center cho phép bắt đầu và dừng Kaspersky Endpoint Security trên một máy khách từ xa, cũng như quản lý và thiết lập cấu hình ứng dụng từ xa.

Chức năng dịch vụ của ứng dụng

Kaspersky Endpoint Security bao gồm một số chức năng dịch vụ. Chức năng dịch vụ có mục đích giúp cập nhật ứng dụng, mở rộng chức năng của ứng dụng, và hỗ trợ người dùng trong việc vận hành ứng dụng.

- **Báo cáo**. Trong quá trình hoạt động, ứng dụng sẽ giữ một bản báo cáo cho mỗi thành phần ứng dụng và tác vụ. Báo cáo chứa một danh sách các sự kiện Kaspersky Endpoint Security và mọi hoạt động mà ứng dụng thực thi. Trong trường hợp xảy ra sự cố, bạn có thể gửi báo cáo đến Kaspersky, ở đó các chuyên gia Hỗ trợ kỹ thuật có thể nhìn vào vấn đề một cách chi tiết hơn.

- **Kho lưu trữ dữ liệu**. Nếu ứng dụng phát hiện các tập tin bị nhiễm virus hoặc có khả năng bị nhiễm virus trong khi quét máy tính để phát hiện virus và các mối đe dọa khác, nó sẽ chặn các tập tin đó. Kaspersky Endpoint Security sẽ di chuyển các tập tin có khả năng bị nhiễm virus đến một ổ lưu trữ đặc biệt gọi là *Cách ly*. Kaspersky Endpoint Security sẽ lưu trữ bản sao của các tập tin đã được khử nhiễm và bị xóa trong *Sao lưu*. Kaspersky Endpoint Security sẽ di chuyển các tập tin không được xử lý vì bất kỳ lý do nào đến *danh sách các tập tin chưa được xử lý*. Bạn có thể quét các tập tin, khôi phục các tập tin về thư mục gốc, và xóa sạch kho lưu trữ dữ liệu.

- **Dịch vụ thông báo**. Dịch vụ thông báo giúp người dùng luôn được cập nhật về trạng thái bảo vệ hiện tại của máy tính và về hoạt động của Kaspersky Endpoint Security. Các thông báo có thể được hiển thị trên màn hình hoặc được gửi qua email.

- **Kaspersky Security Network**. Việc người dùng tham gia vào Kaspersky Security Network sẽ tăng cường hiệu quả bảo vệ máy tính thông qua việc thu thập dữ liệu về danh tiếng các tập tin, tài nguyên web, và phần mềm trong thời gian thực từ người dùng trên toàn thế giới.

- **Bản quyền**. Mua một giấy phép để mở khóa toàn bộ chức năng ứng dụng, cung cấp quyền truy cập đến các bản cập nhật cho cơ sở dữ liệu và mô-đun ứng dụng, và hỗ trợ qua điện thoại hoặc email về các vấn đề liên quan đến việc cài đặt, thiết lập và sử dụng ứng dụng.

- **Hỗ trợ**. Tất cả người dùng đã đăng ký của Kaspersky Endpoint Security đều có thể liên hệ với các chuyên gia của bộ phận Hỗ trợ kỹ thuật để được trợ giúp. Bạn có thể gửi một yêu cầu từ tài khoản My Kaspersky trên website Hỗ trợ kỹ thuật, hoặc nhận hỗ trợ từ chuyên gia qua điện thoại.

Nếu ứng dụng trả về một lỗi hoặc bị treo trong quá trình hoạt động, nó có thể được khởi động lại một cách tự động.

Nếu ứng dụng gặp các lỗi thường xuyên xảy ra và bị sập, ứng dụng sẽ thực hiện hoạt động sau đây:

1. Tắt các chức năng kiểm soát và bảo vệ (chức năng mã hóa vẫn sẽ được bật).

2. Thông báo với người dùng rằng chức năng đã bị tắt.

3. Cố gắng khôi phục ứng dụng về một trạng thái chức năng sau khi cập nhật cơ sở dữ liệu chống virus hoặc áp dụng các bản cập nhật cho mô-đun ứng dụng.

Ứng dụng sẽ nhận thông tin về các lỗi thường xuyên xảy ra và lỗi treo hệ thống sử dụng các thuật toán có mục đích chuyên biệt được quy định bởi các chuyên gia Kaspersky.

Các yêu cầu về phần cứng và phần mềm

Để đảm bảo Kaspersky Endpoint Security có thể hoạt động đúng cách, máy tính của bạn phải đáp ứng được các yêu cầu sau đây:

Cấu hình tối thiểu:

- 2 GB không gian ổ đĩa trống trên ổ cứng
- Bộ vi xử lý với xung nhịp 1 GHz (hỗ trợ bộ chỉ dẫn SSE2)
- RAM:
  - 1 GB đối với hệ điều hành 32 bit;
  - 2 GB đối với hệ điều hành 64 bit.

Các hệ điều hành được hỗ trợ cho máy tính cá nhân:

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 hoặc mới hơn;
- Windows 8 Professional / Enterprise;
- Windows 8.1 Professional / Enterprise;
- Windows 10 Home / Pro / Education / Enterprise.

Để biết thêm chi tiết về việc hỗ trợ cho hệ điều hành Microsoft Windows 10, vui lòng tham khảo Kiến thức cơ bản của Hỗ trợ kỹ thuật.

Các hệ điều hành được hỗ trợ cho máy chủ tập tin:

- Windows Small Business Server 2008 Standard / Premium (64-bit);
- Windows Small Business Server 2011 Essentials / Standard (64-bit);
- Windows MultiPoint Server 2011 (64-bit);
- Windows Server 2008 Standard / Enterprise / Datacenter Service Pack 2 or later;
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 or later;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2019 Essentials / Standard / Datacenter.

Để biết thêm chi tiết về việc hỗ trợ cho hệ điều hành Microsoft Windows Server 2016 và Microsoft Windows Server 2019, vui lòng tham khảo Kiến thức cơ bản của Hỗ trợ kỹ thuật.

Cài đặt và gỡ bỏ ứng dụng

Phần này sẽ hướng dẫn bạn qua quá trình cài đặt Kaspersky Endpoint Security trên máy tính, hoàn tất thiết lập ban đầu, nâng cấp từ một phiên bản cũ của ứng dụng, và gỡ bỏ ứng dụng khỏi máy tính.

Cài đặt ứng dụng

Phần này hướng dẫn cách để cài đặt Kaspersky Endpoint Security trên máy tính của bạn và hoàn tất quá trình thiết lập ban đầu cho ứng dụng.

Thông tin về các cách để cài đặt ứng dụng

Kaspersky Endpoint Security 10 for Windows có thể được cài đặt nội bộ (trực tiếp trên máy tính của người dùng) hoặc từ xa từ máy trạm của quản trị viên.

Việc cài đặt nội bộ Kaspersky Endpoint Security 10 for Windows có thể được thực hiện trong một chế độ sau đây:

- Trong chế độ tương tác bằng cách sử dụng Trình hướng dẫn Cài đặt Ứng dụng.

  Chế độ tương tác yêu cầu ý kiến của bạn trong quá trình cài đặt.

- Trong chế độ im lặng từ dòng lệnh.

  Sau khi tiến trình cài đặt được bắt đầu trong chế độ im lặng, việc tham gia của bạn trong quá trình cài đặt là không cần thiết.

Ứng dụng có thể được cài đặt từ xa trên máy tính mạng sử dụng:

- Bộ phần mềm Kaspersky Security Center (xem *Hướng dẫn Triển khai Kaspersky Security Center*).
- Group Policy Editor của Microsoft Windows (xem các tập tin trợ giúp của hệ điều hành).
- Trình Quản lý Thiết lập Trung tâm Hệ thống.

Chúng tôi khuyến nghị bạn đóng tất cả các ứng dụng đang chạy trước khi bắt đầu cài đặt Kaspersky Endpoint Security (bao gồm cài đặt từ xa).

Cài đặt ứng dụng sử dụng Trình hướng dẫn cài đặt

Giao diện của Trình hướng dẫn Cài đặt ứng dụng bao gồm một chuỗi các cửa sổ tương ứng với các bước cài đặt ứng dụng. Bạn có thể điều hướng giữa các trang của Trình hướng dẫn cài đặt bằng cách sử dụng các nút **Quay lại** và **Tiếp theo**. Để đóng Trình hướng dẫn cài đặt sau khi hoàn thành tác vụ này, nhấn nút **Chấm dứt**. Để dừng Trình hướng dẫn cài đặt ở bất cứ giai đoạn nào, nhấn nút **Hủy bỏ**.

Để cài đặt ứng dụng hoặc nâng cấp ứng dụng từ một phiên bản cũ với Trình hướng dẫn cài đặt:

1. Chạy tập tin setup.exe được bao gồm trong gói phân phối.

Trình hướng dẫn cài đặt sẽ được bắt đầu.

2. Làm theo chỉ dẫn của Trình hướng dẫn cài đặt.

Khi tập tin setup.exe được khởi chạy, Kaspersky Endpoint Security sẽ kiểm tra máy tính để phát hiện bất kỳ phần mềm không tương thích nào. Theo mặc định, khi phát hiện phần mềm không tương thích, quy trình cài đặt sẽ bị hủy bỏ và danh sách các ứng dụng không tương thích với Kaspersky Endpoint Security sẽ xuất hiện trên màn hình. Để tiếp tục cài đặt, gỡ bỏ các ứng dụng này khỏi máy tính.

Bước 1. Đảm bảo máy tính đáp ứng được yêu cầu cài đặt

Trước khi cài đặt Kaspersky Endpoint Security 10 for Windows trên một máy tính hoặc cập nhật một phiên bản cũ của ứng dụng, các điều kiện sau sẽ được kiểm tra:

- Liệu hệ điều hành và gói dịch vụ có đáp ứng được yêu cầu cài đặt sản phẩm về phần mềm hay không.
- Liệu các yêu cầu về phần cứng và phần mềm có được đáp ứng hay không.
- Liệu người dùng có đủ quyền để cài đặt sản phẩm phần mềm hay không.

Nếu bất kỳ điều kiện nào ở trước không được đáp ứng, một thông báo liên quan sẽ được hiển thị trên màn hình.

Nếu máy tính đáp ứng được yêu cầu được liệt kê, Trình hướng dẫn cài đặt sẽ phát hiện các ứng dụng Kaspersky có thể gây xung đột khi chạy ở cùng một thời điểm với trình cài đặt ứng dụng. Nếu các ứng dụng đó được phát hiện, bạn sẽ được nhắc gỡ bỏ chúng một cách thủ công.

Nếu các ứng dụng được phát hiện bao gồm các phiên bản trước đây của Kaspersky Endpoint Security, mọi dữ liệu có thể được di chuyển (ví dụ dữ liệu kích hoạt và thiết lập ứng dụng) đều sẽ được giữ lại và sử dụng trong quá trình cài đặt Kaspersky Endpoint Security 10 Service Pack 2 for Windows, và phiên bản trước đây của ứng dụng sẽ tự động được gỡ bỏ. Chính sách này được áp dụng cho các phiên bản ứng dụng sau đây:

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 CF1 / MP4 CF2
- Kaspersky Anti-Virus 6.0 for Windows Servers MP4 / MP4 CF2
- Kaspersky Endpoint Security 10 Service Pack 1 for Windows
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 for Windows
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 2 for Windows
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 3 for Windows

Bước 2. Trang chào đón đến thủ tục cài đặt

Nếu mọi yêu cầu để cài đặt ứng dụng đã được đáp ứng, một trang chào đón sẽ xuất hiện sau khi bạn khởi chạy gói cài đặt. Trang chào đón sẽ thông báo việc bắt đầu cài đặt Kaspersky Endpoint Security trên máy tính.

Để tiếp tục với Trình hướng dẫn cài đặt, nhấn nút **Tiếp theo**.

Bước 3. Xem Thỏa thuận Giấy phép

Ở bước này, bạn nên xem thỏa thuận giấy phép giữa bạn và Kaspersky.

Đọc kỹ Thỏa thuận Giấy phép và nếu bạn đồng ý với tất cả các điều khoản của giấy phép, chọn hộp kiểm **Tôi chấp nhận các điều khoản của thỏa thuận bản quyền**.

Để quay lại bước trước đó của Trình hướng dẫn cài đặt, nhấn nút **Quay lại**. Để tiếp tục với Trình hướng dẫn cài đặt, nhấn nút **Tiếp theo**. Để dừng Trình hướng dẫn cài đặt, nhấn nút **Hủy bỏ**.

Bước 4. Chọn kiểu cài đặt

Ở bước này, bạn có thể chọn kiểu cài đặt Kaspersky Endpoint Security phù hợp nhất:

- **Cài đặt cơ bản**. Nếu bạn chọn kiểu cài đặt này, các thành phần bảo vệ, Kiểm soát Đặc quyền Ứng dụng và Giám sát Lỗ hổng bảo mật sẽ được cài đặt trên máy tính với những cấu hình được khuyến nghị bởi các chuyên gia Kaspersky.
- **Cài đặt tiêu chuẩn**. Nếu bạn chọn loại cài đặt này, các thành phần bảo vệ và kiểm soát với cấu hình được khuyến nghị bởi Kaspersky sẽ được cài đặt trên máy tính.
- **Cài đặt tùy chỉnh**. Nếu bạn chọn kiểu cài đặt này, bạn sẽ được nhắc để chọn các thành phần được cài đặt và quy định thư mục đích cho ứng dụng.

  Kiểu cài đặt này cho phép bạn cài đặt các thành phần không được bao gồm trong các kiểu cài đặt cơ bản và tiêu chuẩn.

Cài đặt tiêu chuẩn được chọn theo mặc định.

Để quay lại bước trước đó của Trình hướng dẫn cài đặt, nhấn nút **Quay lại**. Để tiếp tục với Trình hướng dẫn cài đặt, nhấn nút **Tiếp theo**. Để dừng Trình hướng dẫn cài đặt, nhấn nút **Hủy bỏ**.

Bước 5. Chọn các thành phần ứng dụng để cài đặt

Bước này được thực thi nếu bạn chọn *Cài đặt tùy chỉnh* ứng dụng.

Ở bước này, bạn có thể chọn các thành phần Kaspersky Endpoint Security mà bạn muốn cài đặt. Chống virus cho tập tin là một thành phần bắt buộc cài đặt. Bạn không thể hủy bỏ việc cài đặt nó.

Theo mặc định, tất cả các thành phần ứng dụng đều được chọn để cài đặt ngoại trừ các thành phần sau:

- Phòng chống Tấn công BadUSB.
- Mã hóa Ổ đĩa.
- Mã hóa Tập tin.
- Quản lý Microsoft BitLocker.

- KATA Endpoint Sensor.

Quản lý Microsoft BitLocker thực hiện các chức năng sau:

- Quản lý mã hóa BitLocker được tích hợp trong hệ điều hành Windows.
- Thiết lập cấu hình chính sách mã hóa và kiểm tra tính khả dụng của chúng trên máy tính được quản lý.
- Bắt đầu các tiến trình mã hóa và giải mã.
- Giám sát tình trạng mã hóa trên máy tính được quản lý.
- Lưu trữ khóa khôi phục trên Máy chủ Quản trị của Kaspersky Security Center.

KATA Endpoint Sensor là một thành phần của Kaspersky Anti Targeted Attack Platform. Giải pháp này được thiết kế để phát hiện nhanh các mối đe dọa như các cuộc tấn công có mục tiêu. Thành phần này sẽ liên tục giám sát các tiến trình, kết nối mạng hoạt động, và các tập tin được sửa đổi, và chuyển tiếp thông tin này đến Kaspersky Anti Targeted Attack Platform.

Để chọn thành phần được cài đặt, nhấn vào biểu tượng cạnh tên thành phần đó để gọi menu ngữ cảnh và chọn **Tính năng này sẽ được cài đặt trên ổ cứng của máy tính**. Để biết thêm chi tiết về các tác vụ được thực hiện bởi thành phần được chọn, và cần bao nhiêu không gian ổ đĩa để cài đặt thành phần đó, hãy xem phần bên dưới của trang Trình hướng dẫn cài đặt hiện tại.

Để xem thông tin chi tiết về không gian khả dụng trên các ổ cứng cục bộ, nhấn nút **Ổ đĩa**. Thông tin sẽ được hiển thị trong cửa sổ **Không gian ổ đĩa khả dụng** được mở ra.

Để hủy bỏ việc cài đặt thành phần, chọn mục **Tính năng sẽ bị vô hiệu hóa** trong menu ngữ cảnh.

Để quay lại danh sách các thành phần được cài đặt mặc định, nhấn nút **Khởi động lại**.

Để quay lại bước trước đó của Trình hướng dẫn cài đặt, nhấn nút **Quay lại**. Để tiếp tục với Trình hướng dẫn cài đặt, nhấn nút **Tiếp theo**. Để dừng Trình hướng dẫn cài đặt, nhấn nút **Hủy bỏ**.

Bước 6. Chọn thư mục đích

Bước này có thể được truy cập nếu bạn chọn *Cài đặt tùy chỉnh* ứng dụng.

Ở bước này, bạn có thể quy định đường dẫn đến thư mục đích có cài đặt ứng dụng. Để chọn thư mục đích cho ứng dụng, nhấn nút **Duyệt**.

Để xem thông tin về không gian khả dụng trên các ổ cứng cục bộ, nhấn nút **Ổ đĩa**. Thông tin sẽ được hiển thị trong cửa sổ **Yêu cầu Không gian Ổ đĩa** được mở ra.

Để quay lại bước trước đó của Trình hướng dẫn cài đặt, nhấn nút **Quay lại**. Để tiếp tục với Trình hướng dẫn cài đặt, nhấn nút **Tiếp theo**. Để dừng Trình hướng dẫn cài đặt, nhấn nút **Hủy bỏ**.

Bước 7. Thêm các mục được loại trừ khỏi tác vụ quét virus

Bước này có thể được truy cập nếu bạn chọn *Cài đặt tùy chỉnh* ứng dụng.

Ở giai đoạn này, bạn có thể thêm vào cấu hình ứng dụng các mục được loại trừ khỏi quét virus.

Các hộp kiểm **Loại trừ các khu vực được khuyến nghị bởi Microsoft khỏi phạm vi quét virus** / **Loại trừ các khu vực được khuyến nghị bởi Kaspersky khỏi phạm vi quét virus** tương ứng sẽ loại trừ các khu vực được khuyến nghị bởi Microsoft hoặc Kaspersky ra khỏi, hoặc bao gồm chúng trong khu vực tin tưởng.

Nếu một trong các hộp kiểm này được lựa chọn, Kaspersky Endpoint Security tương ứng sẽ bao gồm các khu vực được Microsoft hoặc Kaspersky khuyến nghị vào khu vực tin tưởng. Kaspersky Endpoint Security sẽ không quét các khu vực đó để tìm virus và các mối đe dọa khác.

Hộp kiểm **Loại trừ các khu vực được khuyến nghị bởi Microsoft khỏi phạm vi quét virus** có thể được sử dụng khi Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Microsoft Windows cho máy chủ tập tin.

Để quay lại bước trước đó của Trình hướng dẫn cài đặt, nhấn nút **Quay lại**. Để tiếp tục với Trình hướng dẫn cài đặt, nhấn nút **Tiếp theo**. Để dừng Trình hướng dẫn cài đặt, nhấn nút **Hủy bỏ**.

Bước 8. Chuẩn bị cài đặt ứng dụng

Bạn được khuyến nghị bảo vệ tiến trình cài đặt bởi máy tính của bạn có thể bị nhiễm các chương trình độc hại có thể ảnh hưởng đến quá trình cài đặt của Kaspersky Endpoint Security 10 for Windows.

Chức năng bảo vệ tiến trình cài đặt được bật theo mặc định.

Tuy nhiên, nếu ứng dụng không thể được cài đặt (ví dụ, khi thực hiện cài đặt từ xa với sự trợ giúp của Windows Remote Desktop), bạn nên tắt chức năng bảo vệ quy trình cài đặt. Nếu điều này xảy ra, hãy thoát trình cài đặt và bắt đầu lại Trình hướng dẫn Cài đặt Ứng dụng một lần nữa. Ở bước "Chuẩn bị cài đặt ứng dụng", hãy xóa hộp kiểm **Bảo vệ tiến trình cài đặt**.

Hộp kiểm **Đảm bảo tương thích với Citrix PVS** bật / tắc chức năng cài đặt trình điều khiển trong chế độ tương thích với Citrix PVS.

Chỉ chọn hộp kiểm này khi bạn đang làm việc với Citrix Provisioning Services.

Hộp kiểm **Thêm đường dẫn vào tập tin avp.com với biến hệ thống %PATH%** bật / tắt một tùy chọn thêm đường dẫn đến tập tin avp.com vào biến hệ thống %PATH%.

Nếu hộp kiểm này được chọn, việc bắt đầu Kaspersky Endpoint Security hoặc bất kỳ tác vụ nào của ứng dụng từ dòng lệnh sẽ không yêu cầu nhập đường dẫn đến tập tin thực thi. Bạn chỉ cần nhập tên của tập tin thực thi và lệnh sẽ bắt đầu tác vụ đó.

Để quay lại bước trước đó của Trình hướng dẫn cài đặt, nhấn nút **Quay lại**. Để cài đặt chương trình, nhấn nút **Cài đặt**. Để dừng Trình hướng dẫn cài đặt, nhấn nút **Hủy bỏ**.

Kết nối mạng hiện tại có thể được chấm dứt trong khi ứng dụng đang được cài đặt trên máy tính. Hầu hết các kết nối mạng được chấm dứt đều sẽ được khôi phục sau khi việc cài đặt ứng dụng đã hoàn tất.

Bước 9. Cài đặt ứng dụng

Cài đặt của ứng dụng có thể mất một thời gian. Chờ cho nó kết thúc.

Nếu bạn đang cập nhật một phiên bản cũ của ứng dụng, bước này cũng sẽ bao gồm cấu hình di chuyển và gỡ bỏ phiên bản cũ của ứng dụng.

Sau khi tiến trình cài đặt Kaspersky Endpoint Security đã kết thúc, Trình hướng dẫn Thiết lập Ban đầu sẽ được bắt đầu.

Cài đặt ứng dụng từ dòng lệnh

Kaspersky Endpoint Security có thể được cài đặt từ dòng lệnh trong một chế độ sau đây:

- Trong chế độ tương tác bằng cách sử dụng Trình hướng dẫn Cài đặt Ứng dụng.
- Trong chế độ im lặng. Sau khi tiến trình cài đặt được bắt đầu trong chế độ im lặng, việc tham gia của bạn trong quá trình cài đặt là không cần thiết. Để cài đặt ứng dụng trong chế độ im lặng, sử dụng các phím `/s` và `/qn`.

Để cài đặt ứng dụng hoặc nâng cấp phiên bản ứng dụng:

1. Chạy trình biên dịch dòng lệnh (cmd.exe) với tư cách quản trị viên.
2. Tới thư mục chưa bộ cài đặt Kaspersky Endpoint Security.
3. Chạy dòng lệnh sau:

   ```
   setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 [/pKSN=1|0] [/pALLOWREBOOT=1|0] [/pADDLOCAL=<thành phần>] [/pSKIPPRODUCTCHECK=1|0] [/pSKIPPRODUCTUNINSTALL=1|0] [/pKLLOGIN=<tên người dùng> /pKLPASSWD=<mật khẩu> /pKLPASSWDAREA=<phạm vi mật khẩu>] [/pENABLETRACES=1|0 /pTRACESLEVEL=<cấp truy vết>] /s
   ```

   hoặc

   ```
   msiexec /i <tên gói phân phối> EULA=1 PRIVACYPOLICY=1 [KSN=1|0] [ALLOWREBOOT=1|0] [ADDLOCAL=<thành phần>] [SKIPPRODUCTCHECK=1|0] [SKIPPRODUCTUNINSTALL=1|0] [KLLOGIN=<tên người dùng> KLPASSWD=<mật khẩu> KLPASSWDAREA=<phạm vi mật khẩu>] [ENABLETRACES=1|0 TRACESLEVEL=<cấp truy vết>] /qn
   ```

`EULA`	Chấp nhận hoặc từ chối các điều khoản của Thỏa thuận giấy phép người dùng cuối. Giá trị có sẵn: • `1` – chấp nhận các điều khoản của Thỏa thuận giấy phép người dùng cuối. • `0` – từ chối các điều khoản của Thỏa thuận giấy phép người dùng cuối. Văn bản của Thỏa thuận Giấy phép được bao gồm trong gói phân phối của Kaspersky Endpoint Security. Việc chấp nhận các điều khoản của Thỏa thuận giấy phép người dùng cuối là cần thiết để cài đặt ứng dụng hoặc nâng cấp phiên bản ứng dụng.

PRIVACYPOLICY	Chấp nhận hay từ chối Chính sách quyền riêng tư. Giá trị có sẵn: • 1 – chấp nhận Chính sách quyền riêng tư. • 0 – từ chối Chính sách quyền riêng tư. Văn bản của Chính sách quyền riêng tư được bao gồm trong gói phân phối của Kaspersky Endpoint Security. Để cài đặt ứng dụng hoặc nâng cấp ứng dụng phiên bản ứng dụng, bạn phải chấp nhận Chính sách quyền riêng tư.
KSN	Đồng ý hoặc từ chối tham gia Kaspersky Security Network (KSN). Nếu không có giá trị nào được thiết lập cho tham số này, Kaspersky Endpoint Security sẽ nhắc bạn xác nhận sự đồng ý hoặc từ chối tham gia KSN khi Kaspersky Endpoint Security được khởi động lần đầu. Giá trị có sẵn: • 1 – đồng ý tham gia KSN. • 0 – từ chối tham gia KSN (giá trị mặc định). Gói phân phối Kaspersky Endpoint Security được tối ưu cho việc sử dụng với Kaspersky Security Network. Nếu bạn không chọn tham gia Kaspersky Security Network, bạn nên cập nhật Kaspersky Endpoint Security ngay sau khi hoàn tất cài đặt.
ALLOWREBOOT=1	Tự động khởi động lại máy tính nếu cần thiết sau khi cài đặt hoặc nâng cấp ứng dụng. Nếu không có giá trị nào được đặt cho tham số này thì việc tự động khởi động lại máy tính sẽ bị chặn. Không cần khởi động lại khi cài đặt Kaspersky Endpoint Security. Chỉ cần khởi động lại nếu bạn phải gỡ bỏ các ứng dụng không tương thích trước khi cài đặt. Có thể cần khởi động lại khi cập nhật phiên bản ứng dụng.
ADDLOCAL	Chọn các thành phần bổ sung để cài đặt. Theo mặc định, tất cả các thành phần ứng dụng đều được chọn để cài đặt ngoại trừ các thành phần sau: Phòng chống Tấn công BadUSB, Mã hóa mức độ tập tin, Mã hóa toàn bộ ổ đĩa, Quản lý BitLocker và KATA Endpoint Sensor. Giá trị có sẵn: • MSBitLockerFeature. Thành phần Quản lý BitLocker sẽ được cài đặt. • AntiAPTFeature. Thành phần KATA Endpoint Sensor sẽ được cài đặt.
SKIPPRODUCTCHECK=1	Tắt kiểm tra phần mềm không tương thích. Danh sách các phần mềm không tương thích có thể được truy cập trong tập tin incompatible.txt trong gói phân phối. Nếu không có giá trị nào được đặt cho tham số này và phần mềm không tương thích được phát hiện thì quá trình cài đặt Kaspersky Endpoint Security sẽ bị chấm dứt.
SKIPPRODUCTUNINSTALL=1	Tắt tự động gỡ bỏ phần mềm không tương thích được phát hiện. Nếu không có giá trị nào được đặt cho tham số này thì Kaspersky Endpoint Security sẽ cố gắng gỡ bỏ phần mềm không tương thích.
KLLOGIN	Thiết lập tên người dùng để truy cập các tính năng và thiết lập của Kaspersky Endpoint Security (thành phần Mật khẩu). Tên người dùng được quy định cùng với các thiết lập KLPASSWD và KLPASSWDAREA. Tên người dùng mặc định là KLAdmin.

KLPASSWD	Quy định một mật khẩu để truy cập các tính năng và cấu hình của Kaspersky Endpoint Security (mật khẩu được quy định cùng với các tham số KLLOGIN và KLPASSWDAREA). Nếu bạn quy định một mật khẩu nhưng không quy định tên người dùng với tham số KLLOGIN, tên người dùng mặc định KLAdmin sẽ được sử dụng.
KLPASSWDAREA	Quy định phạm vi của mật khẩu để truy cập Kaspersky Endpoint Security. Khi người dùng cố gắng thực hiện một hành động được bao gồm trong phạm vi này, Kaspersky Endpoint Security sẽ hỏi thông tin tài khoản của người dùng (các tham số KLLOGIN và KLPASSWD). Sử dụng ký tự " ; " để nhập nhiều giá trị. Giá trị có sẵn: • SET – sửa đổi thiết lập ứng dụng. • EXIT – thoát ứng dụng. • DISPROTECT – tắt thành phần bảo vệ và dừng tác vụ quét. • DISPOLICY – tắt chính sách Kaspersky Security Center. • UNINST – gỡ bỏ ứng dụng khỏi máy tính. • DISCTRL – tắt các thành phần điều khiển. • REMOVELIC – gỡ bỏ khóa. • REPORTS – xem báo cáo.
ENABLETRACES	Bật hoặc tắt truy vết ứng dụng. Sau khi Kaspersky Endpoint Security khởi động, ứng dụng này sẽ lưu các tập tin dấu vết vào thư mục %ProgramData%/Kaspersky Lab. Giá trị có sẵn: • 1 – dấu vết ứng dụng được bật. • 0 – truy vết bị tắt (giá trị mặc định).
TRACESLEVEL	Cấp chi tiết truy vết. Giá trị có sẵn: • 100 (nghiêm trọng). Chỉ các thông báo lỗi nghiêm trọng. • 200 (cao). Thông báo về tất cả các lỗi, bao gồm lỗi nghiêm trọng. • 300 (chẩn đoán). Thông báo về tất cả các lỗi, và một số thông tin cảnh báo. • 400 (quan trọng). Tất cả các thông báo và cảnh báo về các lỗi thông thường lẫn thiết yếu, và một số thông báo chứa thông tin bổ sung khác. • 500 (bình thường). Tất cả các cảnh báo và thông báo về các lỗi thông thường và thiết yếu, cũng như các thông báo với chi tiết về hoạt động của ứng dụng trong chế độ thông thường (chế độ mặc định). • 600 (thấp). Tất cả thông báo có thể có.

Ví dụ:

```
setup.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1
/pALLOWREBOOT=1 /s

msiexec /i kes_win.msi EULA=1 PRIVACYPOLICY=1
KSN=1 KLLOGIN=Admin KLPASSWD=Password
KLPASSWDAREA=EXIT;DISPOLICY;UNINST /qn

setup.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1
/pENABLETRACES=1 /pTRACESLEVEL=600 /s
```

Sau khi ứng dụng được cài đặt, Kaspersky Endpoint Security sẽ kích hoạt giấy phép dùng thử trừ khi bạn đã nhập một mã kích hoạt vào tập tin setup.ini. Giấy phép dùng thử thường có một thời hạn ngắn. Khi giấy phép dùng thử hết hạn, tất cả các tính năng của Kaspersky Endpoint Security sẽ bị tắt. Để tiếp tục sử dụng ứng dụng, bạn phải kích hoạt một giấy phép thương mại.

Khi cài đặt ứng dụng hoặc nâng cấp phiên bản ứng dụng trong chế độ im lặng, việc sử dụng các tập tin sau đây được hỗ trợ:

- setup.ini – thiết lập cài đặt ứng dụng chung;
- install.cfg – thiết lập cục bộ của Kaspersky Endpoint Security;
- setup.reg – khóa registry.

  Các khóa registry từ tập tin setup.reg chỉ được ghi vào registry nếu giá trị `setup.reg` được quy định cho tham số `SetupReg` trong tập tin setup.ini. Tập tin setup.reg được tạo bởi các chuyên gia Kaspersky. Bạn không nên sửa đổi nội dung của tập tin này.

Để áp dụng thiết lập từ các tập tin setup.ini, install.cfg, và setup.reg, hãy đặt các tập tin này vào thư mục chứa gói phân phối Kaspersky Endpoint Security.

Cài đặt ứng dụng từ xa sử dụng Trình Quản lý Thiết lập Trung tâm Hệ thống

Các hướng dẫn này dành cho Trình Quản lý Thiết lập Trung tâm Hệ thống 2012 R2.

Để cài đặt từ xa một ứng dụng sử dụng Trình Quản lý Thiết lập Trung tâm Hệ thống:

1. Mở bảng điều khiển của Trình Quản lý Thiết lập.
2. Trong phần bên phải của bảng điều khiển, trong mục **Quản lý ứng dụng**, chọn **Gói**.
3. Trong phần trên của bảng điều khiển, trong bảng kiểm soát, nhấn nút **Tạo gói**.

   Việc này sẽ bắt đầu *Trình hướng dẫn Ứng dụng và Gói tin Mới*.
4. Trong Trình hướng dẫn Ứng dụng và Gói tin Mới:

   a. Trong mục **Gói**:

- Trong trường **Tên**, nhập tên của gói cài đặt.
- Trong trường **Thư mục nguồn**, nhập đường dẫn đến thư mục chứa gói phân phối của Kaspersky Endpoint Security.

b. Trong mục **Kiểu ứng dụng**, chọn **Ứng dụng tiêu chuẩn**.

c. Trong mục **Ứng dụng tiêu chuẩn**:

- Trong trường **Tên**, nhập tên đặc trưng cho gói cài đặt (ví dụ, tên ứng dụng bao gồm cả phiên bản).
- Trong trường **Dòng lệnh**, nhập tùy chọn cài đặt của Kaspersky Endpoint Security từ dòng lệnh.
- Nhấn nút **Duyệt** để nhập đường dẫn đến tập tin thực thi của ứng dụng.
- Đảm bảo danh sách **Chế độ thực thi** có mục **Chạy với quyền quản trị viên** được chọn.

d. Trong mục **Yêu cầu**:

- Chọn hộp kiểm **Bắt đầu một ứng dụng khác trước** nếu bạn muốn một ứng dụng khác được khởi chạy trước khi cài đặt Kaspersky Endpoint Security.

  Chọn ứng dụng từ danh sách thả xuống **Ứng dụng** hoặc nhập đường dẫn đến tập tin thực thi của ứng dụng này với nút **Duyệt**.
- Chọn tùy chọn **Ứng dụng này chỉ có thể được bắt đầu trên các nền tảng được quy định** trong mục **Yêu cầu nền tảng** nếu bạn muốn ứng dụng chỉ được cài đặt trong các hệ điều hành được quy định.

  Ở danh sách dưới đây, chọn hộp kiểm đối diện các hệ điều hành sẽ có thể cài đặt Kaspersky Endpoint Security.

Bước này là không bắt buộc.

e. Trong mục **Tóm tắt**, kiểm tra tất cả các giá trị được nhập của cấu hình và nhấn **Tiếp theo**.

Gói cài đặt được tạo sẽ xuất hiện trong mục **Gói** trong danh sách các gói cài đặt khả dụng.

5. Trong menu ngữ cảnh của gói cài đặt, chọn **Triển khai**.

   Việc này sẽ bắt đầu *Trình hướng dẫn Triển khai*.

6. Trong Trình hướng dẫn Triển khai:

   a. Trong mục **Chung**:

   - Trong trường **Phần mềm**, nhập tên đặc trưng của gói cài đặt hoặc chọn gói cài đặt từ danh sách với nút **Duyệt**.
   - Trong trường **Nhóm**, nhập tên của nhóm máy tính mà trên đó sẽ cài đặt ứng dụng, hoặc chọn nhóm này với nút **Duyệt**.

   b. Trong mục **Chứa**, bổ sung các điểm phân phối (để biết thêm chi tiết, vui lòng tham khảo tài liệu trợ giúp cho Trình Quản lý Thiết lập Trung tâm Hệ thống).

   c. Nếu cần thiết, nhập giá trị cho các cấu hình khác trong Trình hướng dẫn Triển khai. Các cấu hình này là không bắt buộc để cài đặt từ xa Kaspersky Endpoint Security.

d. Trong mục **Tóm tắt**, kiểm tra tất cả các giá trị được nhập của cấu hình và nhấn **Tiếp theo**.

Sau khi Trình hướng dẫn Triển khai đã kết thúc, một tác vụ sẽ được tạo để cài đặt từ xa Kaspersky Endpoint Security.

Mô tả thiết lập cài đặt của tập tin setup.ini

Tập tin setup.ini sẽ được sử dụng khi cài đặt ứng dụng từ dòng lệnh, hoặc khi sử dụng Group Policy Editor của Microsoft Windows. Để áp dụng thiết lập từ tập tin setup.ini, hãy đặt tập tin này vào thư mục chứa gói phân phối Kaspersky Endpoint Security.

Tập tin setup.ini bao gồm các phần sau:

- `[Setup]` – các tùy chọn cài đặt ứng dụng chung.
- `[Components]` – lựa chọn các thành phần ứng dụng sẽ được cài đặt. Nếu không có thành phần nào được quy định, tất cả các thành phần khả dụng cho hệ điều hành đều sẽ được cài đặt. Chống virus cho tập tin là một thành phần bắt buộc và được cài đặt trên máy tính bất kể thiết lập được chỉ định trong phần này.
- `[Tasks]` - lựa chọn các tác vụ được bao gồm trong danh sách tác vụ của Kaspersky Endpoint Security. Nếu không có tác vụ nào được quy định, tất cả các tác vụ đều được bao gồm trong danh sách tác vụ của Kaspersky Endpoint Security.

Các giá trị thay thế cho `1` là các giá trị `yes`, `on`, `enable`, và `enabled`.

Các giá trị thay thế cho `0` là các giá trị `no`, `off`, `disable`, và `disabled`.

Các thiết lập của tập tin setup.ini

Phần	Tham số	Mô tả
`[Setup]`	`InstallDir`	Đường dẫn đến thư mục cài đặt ứng dụng.
	`ActivationCode`	Mã kích hoạt Kaspersky Endpoint Security.
	`Eula`	Chấp nhận hoặc từ chối các điều khoản của Thỏa thuận giấy phép người dùng cuối. Giá trị có sẵn: • `1` – chấp nhận các điều khoản của Thỏa thuận giấy phép người dùng cuối. • `0` – từ chối các điều khoản của Thỏa thuận giấy phép người dùng cuối. Văn bản của Thỏa thuận Giấy phép được bao gồm trong gói phân phối của Kaspersky Endpoint Security. Việc chấp nhận các điều khoản của Thỏa thuận giấy phép người dùng cuối là cần thiết để cài đặt ứng dụng hoặc nâng cấp phiên bản ứng dụng.
	`PrivacyPolicy`	Chấp nhận hay từ chối Chính sách quyền riêng

		tư. Giá trị có sẵn: • `1` – chấp nhận Chính sách quyền riêng tư. • `0` – từ chối Chính sách quyền riêng tư. Văn bản của Chính sách quyền riêng tư được bao gồm trong gói phân phối của Kaspersky Endpoint Security. Để cài đặt ứng dụng hoặc nâng cấp ứng dụng phiên bản ứng dụng, bạn phải chấp nhận Chính sách quyền riêng tư.
	`KSN`	Đồng ý hoặc từ chối tham gia Kaspersky Security Network (KSN). Nếu không có giá trị nào được thiết lập cho tham số này, Kaspersky Endpoint Security sẽ nhắc bạn xác nhận sự đồng ý hoặc từ chối tham gia KSN khi Kaspersky Endpoint Security được khởi động lần đầu. Giá trị có sẵn: • `1` – đồng ý tham gia KSN. • `0` – từ chối tham gia KSN (giá trị mặc định). Gói phân phối Kaspersky Endpoint Security được tối ưu cho việc sử dụng với Kaspersky Security Network. Nếu bạn không chọn tham gia Kaspersky Security Network, bạn nên cập nhật Kaspersky Endpoint Security ngay sau khi hoàn tất cài đặt.
	`Login`	Thiết lập tên người dùng để truy cập các tính năng và thiết lập của Kaspersky Endpoint Security (thành phần Mật khẩu). Tên người dùng được quy định cùng với các thiết lập `Password` và `PasswordArea`. Tên người dùng mặc định là KLAdmin.
	`Mật khẩu`	Quy định một mật khẩu để truy cập các tính năng và cấu hình của Kaspersky Endpoint Security (mật khẩu được quy định cùng với các tham số `Login` và `PasswordArea`). Nếu bạn quy định một mật khẩu nhưng không quy định tên người dùng với tham số `Đăng nhập`, tên người dùng mặc định KLAdmin sẽ được sử dụng.
	`PasswordArea`	Quy định phạm vi của mật khẩu để truy cập Kaspersky Endpoint Security. Khi người dùng cố gắng thực hiện một hành động được bao gồm trong phạm vi này, Kaspersky Endpoint Security sẽ hỏi thông tin tài khoản của người dùng (các tham số `Login` và `Password`). Sử dụng ký tự `";"` để nhập nhiều giá trị. Giá trị có sẵn: • `SET` – sửa đổi thiết lập ứng dụng. • `EXIT` – thoát ứng dụng.

		• `DISPROTECT` – tắt thành phần bảo vệ và dừng tác vụ quét. • `DISPOLICY` – tắt chính sách Kaspersky Security Center. • `UNINST` – gỡ bỏ ứng dụng khỏi máy tính. • `DISCTRL` – tắt các thành phần điều khiển. • `REMOVELIC` – gỡ bỏ khóa. • `REPORTS` – xem báo cáo.
	`SelfProtection`	Bật hoặc tắt cơ cấu bảo vệ cài đặt ứng dụng. Giá trị có sẵn: • `1` – Cơ cấu bảo vệ cài đặt ứng dụng được bật. • `0` – cơ cấu bảo vệ cài đặt ứng dụng bị tắt. Bạn có thể tắt chế độ bảo vệ cài đặt. Bảo vệ quá trình cài đặt bao gồm tính năng bảo vệ chống lại nguy cơ thay thế gói phân phối bằng các phần mềm độc hại, chặn truy cập đến thư mục cài đặt của Kaspersky Endpoint Security, và chặn truy cập đến cụm registry hệ thống có chứa các khóa của ứng dụng. Tuy nhiên, nếu ứng dụng không thể được cài đặt (ví dụ, khi thực hiện cài đặt từ xa với sự trợ giúp của Windows Remote Desktop), bạn nên tắt chức năng bảo vệ quy trình cài đặt.
	`Reboot=1`	Tự động khởi động lại máy tính nếu cần thiết sau khi cài đặt hoặc nâng cấp ứng dụng. Nếu không có giá trị nào được đặt cho tham số này thì việc tự động khởi động lại máy tính sẽ bị chặn. Không cần khởi động lại khi cài đặt Kaspersky Endpoint Security. Chỉ cần khởi động lại nếu bạn phải gỡ bỏ các ứng dụng không tương thích trước khi cài đặt. Có thể cần khởi động lại khi cập nhật phiên bản ứng dụng.
	`AddEnvironment`	Biến hệ thống %PATH% sẽ được bổ sung đường dẫn đến các tập tin thực thi trong thư mục cài đặt Kaspersky Endpoint Security. Giá trị có sẵn: • `1` – biến hệ thống %PATH% sẽ được bổ sung đường dẫn đến các tập tin thực thi trong thư mục cài đặt Kaspersky Endpoint Security. • `0` – biến hệ thống %PATH% sẽ không được bổ sung đường dẫn đến các tập tin thực thi trong thư mục cài đặt Kaspersky Endpoint Security.

	AMPPL	Bật hoặc tắt tính năng bảo vệ dịch vụ Kaspersky Endpoint Security bằng công nghệ AM-PPL (Antimalware Protected Process Light). Giá trị có sẵn: • 1 – Tính năng bảo vệ dịch vụ Kaspersky Endpoint Security bằng công nghệ AM-PPL được bật. • 0 – Tính năng bảo vệ dịch vụ Kaspersky Endpoint Security bằng công nghệ AM-PPL bị tắt.
	SetupReg	Cho phép ghi các khóa registry từ tập tin setup.reg vào registry. SetupReg: setup.reg giá trị tham số.
	ENABLETRACES	Bật hoặc tắt truy vết cài đặt ứng dụng. Kaspersky Endpoint Security lưu tập tin dấu vết vào thư mục %ProgramData%/Kaspersky Lab. Giá trị có sẵn: • 1 – truy vết cài đặt ứng dụng được bật. • 0 – truy vết cài đặt ứng dụng bị tắt (giá trị mặc định).
	TracesLevel	Cấp chi tiết truy vết. Giá trị có sẵn: • 100 (nghiêm trọng). Chỉ các thông báo lỗi nghiêm trọng. • 200 (cao). Thông báo về tất cả các lỗi, bao gồm lỗi nghiêm trọng. • 300 (chẩn đoán). Thông báo về tất cả các lỗi, và một số thông tin cảnh báo. • 400 (quan trọng). Tất cả các thông báo và cảnh báo về các lỗi thông thường lẫn thiết yếu, và một số thông báo chứa thông tin bổ sung khác. • 500 (bình thường). Tất cả các cảnh báo và thông báo về các lỗi thông thường và thiết yếu, cũng như các thông báo với chi tiết về hoạt động của ứng dụng trong chế độ thông thường (chế độ mặc định). • 600 (thấp). Tất cả thông báo có thể có.
[Components]	ALL	Cài đặt tất cả các thành phần. Nếu giá trị tham số 1 được quy định, tất cả các thành phần sẽ được cài đặt bất kể cấu hình cài đặt của các thành phần riêng lẻ.
	MailAntiVirus	Chống virus cho thư điện tử.
	IMAntiVirus	Chống virus cho tin nhắn.

	`WebAntiVirus`	Chống virus cho web.
	`ApplicationPrivilegeControl`	Kiểm soát đặc quyền ứng dụng.
	`SystemWatcher`	Giám sát hệ thống.
	`Tường lửa`	Tường lửa.
	`NetworkAttackBlocker`	Ngăn chặn tấn công mạng.
	`WebControl`	Kiểm soát Web.
	`DeviceControl`	Kiểm soát Thiết bị.
	`ApplicationStartupControl`	Kiểm soát Khởi động Ứng dụng.
	`FileEncryption`	Thư viện Mã hóa cấp tập tin.
	`DiskEncryption`	Thư viện Mã hóa toàn bộ ổ đĩa.
	`VulnerabilityAssessment`	Giám sát lỗ hổng bảo mật.
	`KeyboardAuthorization`	Phòng chống Tấn công BadUSB.
	`AntiAPT`	KATA Endpoint Sensor.
	`MSBitLocker`	Quản lý Microsoft BitLocker.
	`AdminKitConnector`	Network Agent Connector để quản trị ứng dụng từ xa thông qua Kaspersky Security Center. Giá trị có sẵn: • `1` – Network Agent Connector được cài đặt. • `0` – Network Agent Connector không được cài đặt.
`[Tasks]`	`ScanMyComputer`	Tác vụ Quét Toàn bộ. Giá trị có sẵn: • `1` – tác vụ này sẽ được bao gồm trong danh sách tác vụ của Kaspersky Endpoint Security. • `0` – tác vụ này không được bao gồm trong danh sách tác vụ của Kaspersky Endpoint Security.
	`ScanCritical`	Tác vụ Quét khu vực quan trọng. Giá trị có sẵn: • `1` – tác vụ này sẽ được bao gồm trong danh sách tác vụ của Kaspersky Endpoint Security. • `0` – tác vụ này không được bao gồm trong danh sách tác vụ của Kaspersky Endpoint Security.
	`Trình cập nhật`	Tác vụ cập nhật. Giá trị có sẵn: • `1` – tác vụ này sẽ được bao gồm trong danh sách tác vụ của Kaspersky Endpoint Security. • `0` – tác vụ này không được bao gồm trong danh sách tác vụ của Kaspersky Endpoint Security.

Trình hướng dẫn Thiết lập Ban đầu

Trình hướng dẫn Thiết lập Ban đầu của Kaspersky Endpoint Security sẽ được bắt đầu khi kết thúc thủ tục cài đặt ứng dụng. Trình hướng dẫn Thiết lập Ban đầu cho phép bạn kích hoạt ứng dụng và thu thập thông tin về các ứng dụng được bao gồm trong hệ điều hành. Các ứng dụng này sẽ được bổ sung vào danh sách các ứng dụng được tin tưởng mà hành động của chúng trong hệ điều hành sẽ không bị bất kỳ hạn chế nào.

Giao diện của Trình hướng dẫn Thiết lập Ban đầu bao gồm nhiều trang (bước) theo trình tự. Bạn có thể điều hướng giữa các trang của Trình hướng dẫn Thiết lập Ban đầu bằng cách sử dụng các nút **Quay lại** và **Tiếp theo**. Để hoàn tất thủ tục của Trình hướng dẫn Thiết lập Ban đầu, nhấn nút **Chấm dứt**. Để dừng thủ tục Trình hướng dẫn Thiết lập Ban đầu ở bất cứ giai đoạn nào, nhấn nút **Hủy bỏ**.

Nếu Trình hướng dẫn Thiết lập Ban đầu bị gián đoạn vì một lý do nào đó, các cấu hình đã được quy định sẽ không được lưu lại. Lần kế tiếp bạn cố gắng sử dụng ứng dụng, Trình hướng dẫn Thiết lập Ban đầu sẽ được bắt đầu một lần nữa, và bạn sẽ phải thiết lập cấu hình từ đầu.

Kích hoạt ứng dụng

Ứng dụng phải được kích hoạt trên một máy tính có ngày và giờ hệ thống được cập nhật. Nếu ngày và giờ hệ thống được thay đổi sau khi kích hoạt ứng dụng, khóa sẽ không thể hoạt động. Ứng dụng sẽ chuyển sang một chế độ hoạt động không có cập nhật, và Kaspersky Security Network sẽ không thể được sử dụng. Key chỉ có thể hoạt động trở lại khi cài đặt lại hệ điều hành.

Ở bước này, chọn một trong các phương án kích hoạt Kaspersky Endpoint Security sau:

- **Kích hoạt với một mã kích hoạt**. Để kích hoạt ứng dụng với một mã kích hoạt, chọn phương án này và nhập một mã kích hoạt.
- **Kích hoạt với tập tin key**. Chọn tùy chọn này để kích hoạt ứng dụng với một tập tin khóa.
- **Kích hoạt phiên bản dùng thử**. Để kích hoạt phiên bản dùng thử của ứng dụng, chọn phương án này. Người dùng có thể sử dụng phiên bản đầy đủ chức năng của ứng dụng trong thời hạn được giới hạn bởi giấy phép cho phiên bản dùng thử của ứng dụng. Sau khi giấy phép hết hạn, chức năng của ứng dụng sẽ bị chặn và bạn không thể kích hoạt phiên bản dùng thử một lần nữa.
- **Kích hoạt sau**. Chọn phương án này nếu bạn muốn bỏ qua bước kích hoạt Kaspersky Endpoint Security. Người dùng sẽ chỉ có thể làm việc với các thành phần Chống virus cho tập tin và Tường lửa. Người dùng sẽ có thể cập nhật cơ sở dữ liệu chống virus và mô-đun của Kaspersky Endpoint Security một lần sau cài đặt. Phương án **Kích hoạt sau** chỉ có thể được sử dụng sau lần khởi động đầu tiên của Trình hướng dẫn Thiết lập Ban đầu, ngay sau khi cài đặt ứng dụng.

Cần có kết nối Internet để kích hoạt phiên bản dùng thử của ứng dụng, hoặc để kích hoạt ứng dụng với một mã kích hoạt.

Để tiếp tục với Trình hướng dẫn Thiết lập Ban đầu, chọn một phương án nâng cao và nhấn nút **Tiếp theo**. Để dừng Trình hướng dẫn Thiết lập Ban đầu, nhấn nút **Hủy bỏ**.

Kích hoạt với một mã kích hoạt

Bước này chỉ có thể được sử dụng khi bạn kích hoạt ứng dụng với một mã kích hoạt. Bước này sẽ được bỏ qua khi bạn kích hoạt phiên bản dùng thử của ứng dụng hoặc khi bạn kích hoạt ứng dụng với một tập tin khóa.

Trong bước này, Kaspersky Endpoint Security sẽ gửi dữ liệu đến máy chủ kích hoạt để xác minh mã kích hoạt được nhập:

- Nếu mã kích hoạt được xác minh thành công, Trình hướng dẫn Thiết lập Ban đầu sẽ tự động chuyển sang cửa sổ tiếp theo.
- Nếu việc xác minh mã kích hoạt thất bại, một thông báo tương ứng sẽ xuất hiện. Trong trường hợp này, bạn nên tìm kiếm lời khuyên từ nhà cung cấp phần mềm đã bán cho bạn giấy phép sử dụng Kaspersky Endpoint Security.
- Nếu số lượt kích hoạt với mã kích hoạt vượt quá một mức nhất định, một thông báo tương ứng sẽ xuất hiện. Trình hướng dẫn Thiết lập Ban đầu sẽ bị gián đoạn, và ứng dụng sẽ đề nghị bạn liên hệ với bộ phận Hỗ trợ kỹ thuật của Kaspersky.

Để quay lại bước trước đó của Trình hướng dẫn Thiết lập Ban đầu, nhấn nút **Quay lại**. Để dừng Trình hướng dẫn Thiết lập Ban đầu, nhấn nút **Hủy bỏ**.

Kích hoạt với một tập tin khóa

Bước này chỉ có thể được sử dụng khi bạn kích hoạt ứng dụng với một tập tin khóa.

Ở bước này, nhập đường dẫn đến tập tin khóa. Để làm điều đó, nhấn nút **Duyệt** và chọn một tập tin khóa của biểu mẫu `<File ID>.key`.

Sau khi bạn đã chọn một tập tin khóa, các thông tin sau sẽ được hiển thị ở phần dưới của cửa sổ:

- Khóa
- Kiểu giấy phép (thương mại hoặc dùng thử) và số máy tính được bao gồm trong giấy phép này
- Ngày kích hoạt ứng dụng trên máy tính
- Ngày hết hạn giấy phép
- Chức năng ứng dụng khả dụng theo giấy phép
- Thông báo về các vấn đề liên quan đến khóa, nếu có. Ví dụ, *Danh sách đen các khóa bị hỏng*.

Để quay lại bước trước đó của Trình hướng dẫn Thiết lập Ban đầu, nhấn nút **Quay lại**. Để tiếp tục với Trình hướng dẫn Thiết lập Ban đầu, nhấn nút **Tiếp theo**. Để dừng Trình hướng dẫn Thiết lập Ban đầu, nhấn nút **Hủy bỏ**.

Chọn các chức năng để kích hoạt

Bước này chỉ có thể được sử dụng khi bạn kích hoạt phiên bản dùng thử của ứng dụng.

Ở bước này, bạn có thể lựa chọn chức năng sẽ được cung cấp sau khi kích hoạt ứng dụng:

- **Cài đặt cơ bản**. Nếu tùy chọn này được chọn, chỉ các thành phần bảo vệ, Kiểm soát Đặc quyền Ứng dụng và Giám sát Lỗ hổng bảo mật là được cung cấp sau khi kích hoạt ứng dụng.
- **Cài đặt tiêu chuẩn**. Nếu tùy chọn này được chọn, chỉ các thành phần bảo vệ và kiểm soát của ứng dụng sẽ được cung cấp sau khi kích hoạt ứng dụng.
- **Cài đặt đầy đủ**. Nếu tùy chọn này được chọn, tất cả các thành phần ứng dụng được cài đặt, bao gồm chức năng mã hóa dữ liệu đều sẽ được cung cấp sau khi kích hoạt ứng dụng.

Nếu bạn đã chọn nhiều thành phần hơn số lượng cho phép của giấy phép trong quá trình cài đặt, sau khi kích hoạt ứng dụng, các thành phần không được cung cấp theo giấy phép sẽ được cài đặt nhưng không thể được sử dụng. Nếu giấy phép đã mua cho phép nhiều thành phần hơn là đang được cài đặt, sau khi ứng dụng được cài đặt, các thành phần chưa được cài đặt sẽ được liệt kê trong mục **Bản quyền**.

Cài đặt tiêu chuẩn được chọn theo mặc định.

Để quay lại bước trước đó của Trình hướng dẫn Thiết lập Ban đầu, nhấn nút **Quay lại**. Để tiếp tục với Trình hướng dẫn Thiết lập Ban đầu, nhấn nút **Tiếp theo**. Để dừng Trình hướng dẫn Thiết lập Ban đầu, nhấn nút **Hủy bỏ**.

Hoàn thành kích hoạt

Trong bước này, Trình hướng dẫn Thiết lập Ban đầu sẽ thông báo cho bạn về việc kích hoạt thành công Kaspersky Endpoint Security. Thông tin sau đây về giấy phép sẽ được cung cấp:

- Kiểu giấy phép (thương mại hoặc dùng thử) và số máy tính được bao gồm trong giấy phép này
- Ngày hết hạn giấy phép
- Chức năng ứng dụng khả dụng theo giấy phép

Để tiếp tục với Trình hướng dẫn Thiết lập Ban đầu, nhấn nút **Tiếp theo**. Để dừng Trình hướng dẫn Thiết lập Ban đầu, nhấn nút **Hủy bỏ**.

Phân tích hệ điều hành

Ở bước này, thông tin sẽ được thu thập về các ứng dụng được bao gồm trong hệ điều hành. Các ứng dụng này sẽ được bổ sung vào danh sách các ứng dụng được tin tưởng mà hành động của chúng trong hệ điều hành sẽ không bị bất kỳ hạn chế nào.

Các ứng dụng khác sẽ được phân tích khi chúng được khởi động lần đầu tiên sau khi Kaspersky Endpoint Security đã được cài đặt.

Để dừng Trình hướng dẫn Thiết lập Ban đầu, nhấn nút **Hủy bỏ**.

Hoàn tất thiết lập ban đầu cho ứng dụng

Cửa sổ hoàn tất Trình hướng dẫn Thiết lập Ban đầu chứa thông tin về việc hoàn tất tiến trình cài đặt của Kaspersky Endpoint Security.

Nếu bạn muốn khởi động Kaspersky Endpoint Security, nhấn nút **Hoàn tất**.

Nếu bạn muốn thoát Trình hướng dẫn Thiết lập Ban đầu mà không khởi động Kaspersky Endpoint Security, xóa hộp kiểm **Bắt đầu Kaspersky Endpoint Security 10 for Windows** và nhấn nút **Hoàn tất**.

Tuyên bố Kaspersky Security Network

Trong bước này, bạn được mời tham gia vào Kaspersky Security Network.

Để xem lại Tuyên bố Kaspersky Security Network:

- Nếu bạn chấp nhận tất cả các điều khoản, chọn mục **Tôi chấp nhận các điều khoản tham gia Kaspersky Security Network** trong cửa sổ của Trình hướng dẫn Thiết lập Ban đầu.
- Nếu bạn không chấp nhận tất cả các điều khoản tham gia Kaspersky Security Network, chọn mục **Tôi không chấp nhận các điều khoản tham gia Kaspersky Security Network** trong cửa sổ của Trình hướng dẫn Thiết lập Ban đầu.

Để tiếp tục Trình hướng dẫn Thiết lập Ban đầu, nhấn **OK**.

Thông tin về các cách để nâng cấp một phiên bản ứng dụng cũ

Để nâng cấp một phiên bản cũ của ứng dụng lên Kaspersky Endpoint Security 10 Service Pack 2 for Windows, hãy giải mã tất cả các ổ cứng được mã hóa.

Bạn có thể nâng cấp các ứng dụng sau đây lên Kaspersky Endpoint Security 10 Service Pack 2 for Windows:

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4 CF1 (bản dựng 6.0.4.1424) / MP4 CF2 (bản dựng 6.0.4.1611)
- Kaspersky Anti-Virus 6.0 for Windows Servers MP4 (bản dựng 6.0.4.1424) / MP4 CF2 (bản dựng 6.0.4.1611)
- Kaspersky Endpoint Security 10 Service Pack 1 for Windows (bản dựng 10.2.2.10535)
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 1 for Windows (bản dựng 10.2.2.10535(MR1))

- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 2 for Windows (bản dựng 10.2.4.674)
- Kaspersky Endpoint Security 10 Service Pack 1 Maintenance Release 3 for Windows (bản dựng 10.2.5.3201).

Khi bất kỳ một ứng dụng nào được liệt kê trên đây được nâng cấp lên Kaspersky Endpoint Security 10 Service Pack 2 for Windows, nội dung của Cách ly và Sao lưu sẽ không được chuyển tiếp.

Bạn có thể nâng cấp phiên bản cũ của ứng dụng như sau:

- Trên máy tính trong chế độ tương tác bằng cách sử dụng Trình hướng dẫn Cài đặt Ứng dụng.
- Nội bộ trong chế độ phi tương tác sử dụng dòng lệnh
- Từ xa sử dụng bộ phần mềm Kaspersky Security Center (xem *Hướng dẫn Triển khai Kaspersky Security Center*).
- Từ xa sử dụng Group Policy Editor của Microsoft Windows (xem các tập tin trợ giúp của hệ điều hành)

Khi nâng cấp một phiên bản cũ của ứng dụng lên Kaspersky Endpoint Security 10 Service Pack 2 for Windows, bạn không cần phải gỡ bỏ phiên bản cũ của ứng dụng. Chúng tôi khuyến nghị bạn thoát tất cả các ứng dụng đang hoạt động trước khi nâng cấp một phiên bản cũ của ứng dụng.

Gỡ bỏ ứng dụng

Phần này mô tả cách bạn có thể gỡ bỏ Kaspersky Endpoint Security khỏi máy tính.

Thông tin về các cách để gỡ bỏ ứng dụng

Việc gỡ bỏ Kaspersky Endpoint Security sẽ khiến máy tính và dữ liệu người dùng không được bảo vệ chống lại các mối đe dọa.

Kaspersky Endpoint Security có thể được gỡ bỏ khỏi máy tính theo một số cách:

- Nội bộ trong chế độ tương tác bằng cách sử dụng Trình hướng dẫn cài đặt
- Nội bộ trong chế độ phi tương tác sử dụng dòng lệnh
- Từ xa sử dụng bộ phần mềm Kaspersky Security Center (xem *Hướng dẫn Triển khai Kaspersky Security Center* để biết thêm chi tiết)
- Từ xa sử dụng Group Policy Editor của Microsoft Windows (xem các tập tin trợ giúp của hệ điều hành)

Gỡ bỏ ứng dụng bằng cách sử dụng Trình hướng dẫn cài đặt.

Để gỡ bỏ Kaspersky Endpoint Security bằng cách sử dụng Trình hướng dẫn cài đặt:

1. Trong menu **Start**, chọn **Applications → Kaspersky Endpoint Security 10 for Windows → Modify, Repair, or Remove**.

   Trình hướng dẫn cài đặt sẽ được bắt đầu.

2. Trong cửa sổ **Thay đổi, Sửa chữa, hoặc Gỡ bỏ ứng dụng** của Trình hướng dẫn cài đặt, nhấn nút **Gỡ bỏ**.

3. Làm theo chỉ dẫn của Trình hướng dẫn cài đặt.

Bước 1. Lưu dữ liệu ứng dụng để sử dụng trong tương lai

Trong bước này, bạn có thể chỉ định các dữ liệu được sử dụng bởi các ứng dụng mà bạn muốn giữ lại để sử dụng thêm trong khi cài đặt tiếp theo của ứng dụng (ví dụ, khi cài đặt một phiên bản mới hơn). Nếu bạn không quy định bất cứ dữ liệu nào, ứng dụng sẽ bị gỡ bỏ hoàn toàn.

Để lưu dữ liệu ứng dụng để sử dụng trong tương lai,

chọn các hộp kiểm cạnh kiểu dữ liệu mà bạn muốn lưu lại:

- **Dữ liệu kích hoạt** - dữ liệu loại bỏ sự cần thiết của việc kích hoạt ứng dụng được bạn cài đặt trong tương lai. Nó sẽ tự động được kích hoạt theo giấy phép hiện tại, chừng nào giấy phép chưa hết hạn tính đến thời điểm cài đặt.

- **Tập tin Sao lưu và Cách ly** - các tập tin được quét bởi ứng dụng và đặt trong Sao lưu hoặc Cách ly.

  Các tập tin Sao lưu và Cách ly được lưu sau khi gỡ bỏ ứng dụng chỉ có thể được truy cập từ cùng một phiên bản ứng dụng đã được sử dụng để lưu các tập tin đó.

  Nếu bạn muốn sử dụng các đối tượng Sao lưu và Cách ly sau khi gỡ bỏ ứng dụng, bạn phải khôi phục các đối tượng đó từ kho lưu trữ của chúng trước khi gỡ bỏ ứng dụng. Tuy nhiên, các chuyên gia Kaspersky không khuyến nghị việc khôi phục ứng dụng từ Sao lưu và Cách ly bởi điều đó có thể gây hại cho máy tính.

- **Cấu hình hoạt động của ứng dụng** - giá trị của các cấu hình ứng dụng được chọn trong quá trình thiết lập ứng dụng.

- **Nơi lưu trữ khóa mã hóa** - dữ liệu cho phép truy cập trực tiếp đến các tập tin và thiết bị được mã hóa trước khi gỡ bỏ ứng dụng. Các tập tin và thiết bị được mã hóa có thể được truy cập trực tiếp sau khi ứng dụng được cài đặt lại với chức năng mã hóa.

  Hộp kiểm này được chọn theo mặc định.

Để tiếp tục với Trình hướng dẫn cài đặt, nhấn nút **Tiếp theo**. Để dừng Trình hướng dẫn cài đặt, nhấn nút **Hủy bỏ**.

Bước 2. Xác nhận gỡ bỏ ứng dụng

Bởi việc gỡ bỏ ứng dụng có thể phức tạp hóa việc bảo mật cho máy tính của bạn, bạn sẽ được yêu cầu xác nhận quyết định gỡ bỏ ứng dụng. Để làm điều này, nhấn nút **Gỡ bỏ**.

Để dừng thủ tục gỡ bỏ ứng dụng bất cứ lúc nào, bạn có thể hủy bỏ hoạt động này bằng cách nhấn nút **Hủy bỏ**.

Bước 3. Gỡ bỏ ứng dụng. Hoàn tất gỡ bỏ

Trong bước này, Trình hướng dẫn cài đặt sẽ gỡ bỏ ứng dụng khỏi máy tính của bạn. Đợi cho đến khi quá trình gỡ bỏ ứng dụng đã hoàn tất.

Khi gỡ bỏ ứng dụng, hệ điều hành của bạn có thể sẽ cần được khởi động lại. Nếu bạn không muốn khởi động lại ngay, việc hoàn tất thủ tục gỡ bỏ ứng dụng sẽ được hoãn cho đến khi hệ điều hành đã được khởi động lại, hoặc đến khi máy tính được tắt và sau đó được bật lại.

Gỡ bỏ ứng dụng từ dòng lệnh

Bạn có thể bắt đầu tiến trình gỡ bỏ ứng dụng từ dòng lệnh. Việc gỡ bỏ được thực hiện trong chế độ tương tác hoặc im lặng (mà không cần khởi động Trình hướng dẫn Cài đặt Ứng dụng).

Để bắt đầu tiến trình gỡ bỏ ứng dụng trong chế độ tương tác,

trong dòng lệnh nhập `setup.exe /x` hoặc `msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275}`.

Trình hướng dẫn cài đặt sẽ được bắt đầu. Làm theo chỉ dẫn của Trình hướng dẫn cài đặt.

Để bắt đầu tiến trình gỡ bỏ ứng dụng trong chế độ im lặng,

trong dòng lệnh nhập `setup.exe /s /x` or `msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275} /qn`.

Việc này sẽ bắt đầu tiến trình gỡ bỏ ứng dụng trong chế độ im lặng (mà không khởi động Trình hướng dẫn cài đặt).

Nếu hoạt động gỡ bỏ ứng dụng được bảo vệ bởi mật khẩu, tên người dùng và mật khẩu tương ứng phải được nhập vào dòng lệnh.

Để gỡ bỏ ứng dụng khỏi dòng lệnh trong chế độ tương tác khi tên người dùng và mật khẩu xác thực việc gỡ bỏ, thay đổi hoặc sửa chữa Kaspersky Endpoint Security đã được đặt:

Trong dòng lệnh, nhập `setup.exe /pKLLOGIN=<Tên người dùng> /pKLPASSWD=***** /x` hoặc

`msiexec.exe KLLOGIN=<Tên người dùng> KLPASSWD=***** /x {7911E943-32CC-45D0-A29C-56E6EF762275}`.

Trình hướng dẫn cài đặt sẽ được bắt đầu. Làm theo chỉ dẫn của Trình hướng dẫn cài đặt.

Để gỡ bỏ ứng dụng khỏi dòng lệnh trong chế độ im lặng khi tên người dùng và mật khẩu xác thực việc gỡ bỏ, thay đổi hoặc sửa chữa Kaspersky Endpoint Security đã được đặt:

Trong dòng lệnh, nhập `setup.exe /pKLLOGIN=<Tên người dùng> /pKLPASSWD=***** /s /x` hoặc

```
msiexec.exe /x {7911E943-32CC-45D0-A29C-56E6EF762275} KLLOGIN=<Tên người dùng>
KLPASSWD=***** /qn.
```

Xóa các đối tượng và dữ liệu còn sót lại sau hoạt động thử nghiệm của Authentication Agent

Trong quá trình gỡ bỏ ứng dụng, nếu Kaspersky Endpoint Security phát hiện các đối tượng và dữ liệu còn trên ổ cứng hệ thống sau hoạt động thử nghiệm của Authentication Agent, việc gỡ bỏ ứng dụng sẽ bị gián đoạn và không thể được thực hiện cho đến khi các đối tượng và dữ liệu đó đã được gỡ bỏ.

Các đối tượng và dữ liệu chỉ được lưu trên ổ cứng hệ thống sau hoạt động thử nghiệm của Authentication Agent trong các trường hợp ngoại lệ. Ví dụ, điều này có thể xảy ra nếu máy tính chưa được khởi động lại sau khi một chính sách Kaspersky Security Center với cấu hình mã hóa đã được áp dụng, hoặc nếu ứng dụng không thể khởi động sau hoạt động thử nghiệm của Authentication Agent.

Bạn có thể xóa các đối tượng và dữ liệu còn trên ổ cứng hệ thống sau hoạt động thử nghiệm của Authentication Agent bằng hai cách:

- Sử dụng chính sách Kaspersky Security Center.
- Sử dụng Tiện ích Khôi phục.

Để sử dụng một chính sách Kaspersky Security Center và xóa các đối tượng và dữ liệu còn sót lại sau hoạt động thử nghiệm của Authentication Agent:

1. Áp dụng một chính sách Kaspersky Security Center cho máy tính với cấu hình được thiết lập để giải mã toàn bộ ổ cứng của máy tính.
2. Bắt đầu Kaspersky Endpoint Security.

Để sử dụng Tiện ích Khôi phục và xóa các đối tượng và dữ liệu còn sót lại sau hoạt động thử nghiệm của Authentication Agent:

1. Bắt đầu Tiện ích Khôi phục bằng cách chạy tập tin thực thi fdert.exe được tạo với Kaspersky Endpoint Security trên máy tính với ổ cứng hệ thống được kết nối mà trên đó còn sót lại các đối tượng và dữ liệu sau hoạt động thử nghiệm của authentication agent.
2. Trong danh sách thả xuống **Lựa chọn thiết bị** trong cửa sổ của Tiện ích Khôi phục, chọn ổ cứng hệ thống với các đối tượng và dữ liệu cần được xóa.
3. Nhấn nút **Quét**.
4. Nhấn nút **Xóa các đối tượng AA và dữ liệu**.

Việc này sẽ bắt đầu một tiến trình để xóa các đối tượng và dữ liệu còn sót lại sau hoạt động thử nghiệm của Authentication Agent.

Sau khi đã xóa các đối tượng và dữ liệu còn sót lại sau hoạt động thử nghiệm của Authentication Agent, bạn có thể sẽ cần xóa thêm thông tin về tính không tương thích của ứng dụng với Authentication Agent.

Để xóa thông tin về tính không tương thích của ứng dụng với Authentication Agent,

nhập lệnh `avp pbatestreset` vào dòng lệnh.

Các thành phần mã hóa phải được cài đặt để lệnh `avp pbatestreset` có thể được thực thi.

Giao diện ứng dụng

Mục này mô tả các thành phần chính trong giao diện ứng dụng.

Biểu tượng ứng dụng trong khu vực thông báo trên thanh tác vụ

Ngay sau khi cài đặt Kaspersky Endpoint Security, biểu tượng của ứng dụng sẽ xuất hiện trong khu vực thông báo trên thanh tác vụ Microsoft Windows.

Biểu tượng này có các mục đích sau:

- Nó thể hiện hoạt động của ứng dụng.
- Nó có vai trò như một đường dẫn tắt đến menu ngữ cảnh và cửa sổ chính của ứng dụng.

Chỉ báo hoạt động của ứng dụng

Biểu tượng ứng dụng có vai trò như một chỉ báo cho hoạt động của ứng dụng:

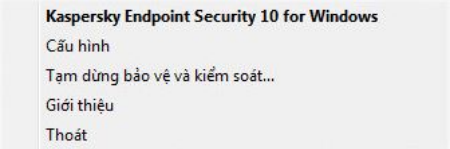
- Biểu tượng thể hiện rằng tất cả các thành phần bảo vệ của ứng dụng đều được bật.
- Biểu tượng thể hiện rằng đã xảy ra các sự kiện quan trọng cần sự chú ý của bạn trong hoạt động của Kaspersky Endpoint Security. Ví dụ, Chống virus cho tập tin đã bị tắt hoặc cơ sở dữ liệu ứng dụng đã bị lỗi thời.
- Biểu tượng thể hiện rằng đã xảy ra các sự kiện thiết yếu trong hoạt động của Kaspersky Endpoint Security. Ví dụ, có lỗi trong hoạt động của một thành phần, hoặc hỏng cơ sở dữ liệu ứng dụng.

Menu ngữ cảnh của biểu tượng ứng dụng

Menu ngữ cảnh của biểu tượng ứng dụng chứa các mục sau đây:

- **Kaspersky Endpoint Security 10 for Windows**. Mở thẻ **Bảo vệ và Kiểm soát** trong cửa sổ chính của ứng dụng. Thẻ **Bảo vệ và Kiểm soát** cho phép bạn điều chỉnh hoạt động của các thành phần và tác vụ của ứng dụng, và xem số liệu thống kê các tập tin được xử lý và mối đe dọa được phát hiện.
- **Cấu hình**. Mở thẻ **Cấu hình** trong cửa sổ chính của ứng dụng. Thẻ **Cấu hình** cho phép bạn thay đổi các cấu hình ứng dụng mặc định.
- **Tạm ngưng bảo vệ và kiểm soát** / **Khôi phục bảo vệ và kiểm soát**. Tạm ngưng / khôi phục hoạt động của các thành phần bảo vệ và kiểm soát. Mục menu ngữ cảnh này không ảnh hưởng đến các tác vụ cập nhật và tác vụ quét, chỉ khả dụng khi chính sách Kaspersky Security Center bị tắt.
- **Tắt chính sách** / **Bật chính sách**. Tắt / bật chính sách Kaspersky Security Center. Mục menu ngữ cảnh này có thể được sử dụng khi Kaspersky Endpoint Security hoạt động theo một chính sách, và một mật khẩu để tắt chính sách Kaspersky Security Center đã được thiết lập.
- **Giới thiệu**. Mục này mở ra một cửa sổ thông tin với các chi tiết của ứng dụng.

- **Thoát**. Mục này sẽ đóng Kaspersky Endpoint Security. Nhấn vào mục menu ngữ cảnh để giải phóng ứng dụng khỏi RAM máy tính.



Menu ngữ cảnh của biểu tượng ứng dụng

Bạn có thể mở menu ngữ cảnh của biểu tượng ứng dụng bằng cách đặt con trỏ lên biểu tượng ứng dụng trong khu vực thông báo trên thanh tác vụ của Microsoft Windows và nhấn nút phải chuột.

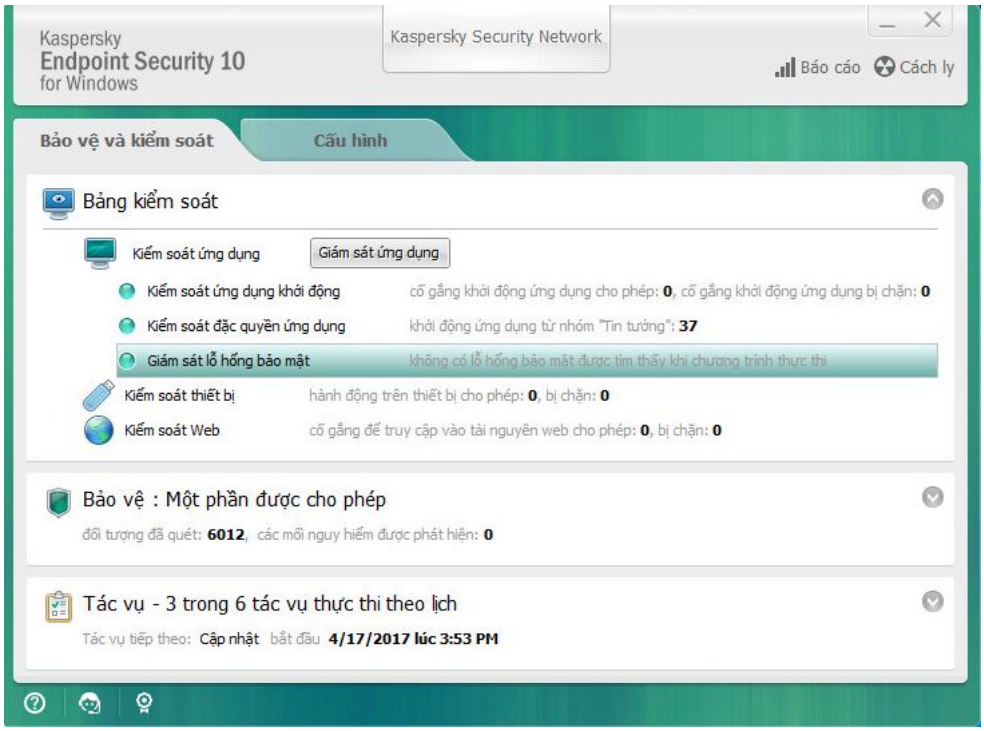
Cửa sổ chính của ứng dụng

Cửa sổ chính của Kaspersky Endpoint Security chứa các thành phần giao diện cung cấp quyền truy cập đến các chức năng chính của ứng dụng.

Cửa sổ chính của ứng dụng được chia làm bốn phần (xem hình dưới đây):

- Phần trên của cửa sổ chứa các thành phần giao diện cho phép bạn xem thông tin sau đây:
  - Chi tiết ứng dụng
  - Thống kê Kaspersky Security Network
  - Danh sách các tập tin chưa được xử lý
  - Danh sách các lỗ hổng bảo mật được phát hiện
  - Danh sách các tập tin được cách ly
  - Kho lưu trữ bản sao của các tập tin bị nhiễm virus đã được ứng dụng xóa
  - Báo cáo về các sự kiện đã xảy ra trong quá trình hoạt động tổng quát của ứng dụng hoặc của các thành phần riêng biệt, hoặc trong quá trình thực thi tác vụ
- Thẻ **Bảo vệ và Kiểm soát** cho phép bạn điều chỉnh hoạt động của các thành phần ứng dụng và việc hoàn tất các tác vụ. Thẻ **Bảo vệ và Kiểm soát** được hiển thị khi bạn mở cửa sổ chính của ứng dụng.
- Thẻ **Cấu hình** cho phép bạn sửa các cấu hình ứng dụng mặc định.
- Phần dưới của cửa sổ chứa các thành phần sau đây:
  - **Nút** . Nhấn vào nút này để chuyển đến hệ thống trợ giúp của Kaspersky Endpoint Security.
  - **Nút** . Nhấn vào nút này để mở ra cửa sổ **Hỗ trợ**, có chứa thông tin về hệ điều hành, phiên bản hiện tại của Kaspersky Endpoint Security và liên kết đến các tài nguyên thông tin của Kaspersky.
  - **Nút** / . Nhấn vào nút này để mở ra cửa sổ **Bản quyền** với thông tin về giấy phép hiện tại.
  - **Nút** / / Nhấn vào nút này để mở ra cửa sổ **Sự kiện** chứa thông tin về các bản cập nhật khả dụng cũng như các yêu cầu truy cập vào tập tin và thiết bị.

    Nút này chỉ khả dụng khi có các yêu cầu truy cập hoặc bản cập nhật bị gỡ bỏ.



Cửa sổ chính của ứng dụng

Để mở cửa sổ chính của Kaspersky Endpoint Security, thực hiện một trong các thao tác sau:

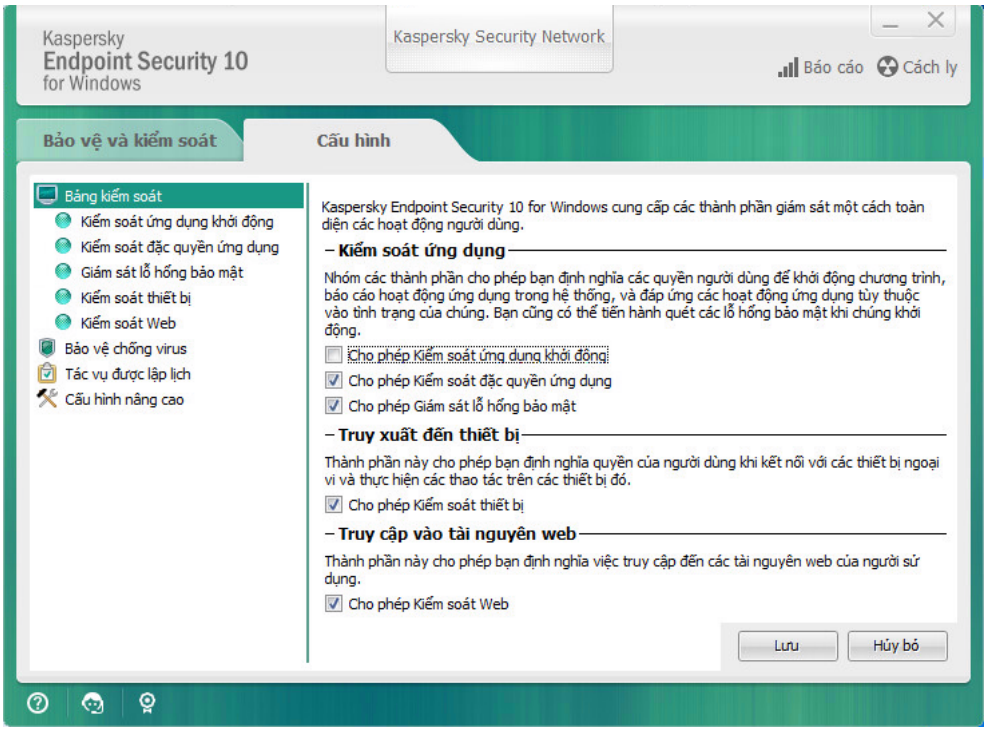
- Nhấn vào biểu tượng ứng dụng trong khu vực thông báo trên thanh tác vụ của Microsoft Windows.
- Chọn **Kaspersky Endpoint Security 10 for Windows** trong menu ngữ cảnh của biểu tượng ứng dụng.

Thẻ Thiết lập cấu hình ứng dụng

Thẻ cấu hình Kaspersky Endpoint Security cho phép bạn thiết lập các cấu hình chung của ứng dụng, các thành phần riêng lẻ, báo cáo và lưu trữ, các tác vụ quét, tác vụ cập nhật, tác vụ quét lỗ hổng bảo mật, và giao tiếp với máy chủ Kaspersky Security Network.

Thẻ cấu hình ứng dụng bao gồm hai phần (xem hình dưới đây):

- Phần bên trái chứa các thành phần ứng dụng, tác vụ, và một mục cấu hình nâng cao bao gồm nhiều mục con.
- Phần bên phải chứa các thành phần kiểm soát mà bạn có thể sử dụng để thiết lập cấu hình của thành phần hoặc tác vụ được lựa chọn ở phần bên trái của cửa sổ, cũng như các cấu hình nâng cao.



Thẻ Thiết lập cấu hình ứng dụng

Để mở thẻ cấu hình ứng dụng, thực hiện một trong các thao tác sau:

- Trong cửa sổ chính của ứng dụng, chọn thẻ **Cấu hình**.
- Trong menu ngữ cảnh của biểu tượng ứng dụng, chọn **Cấu hình**.

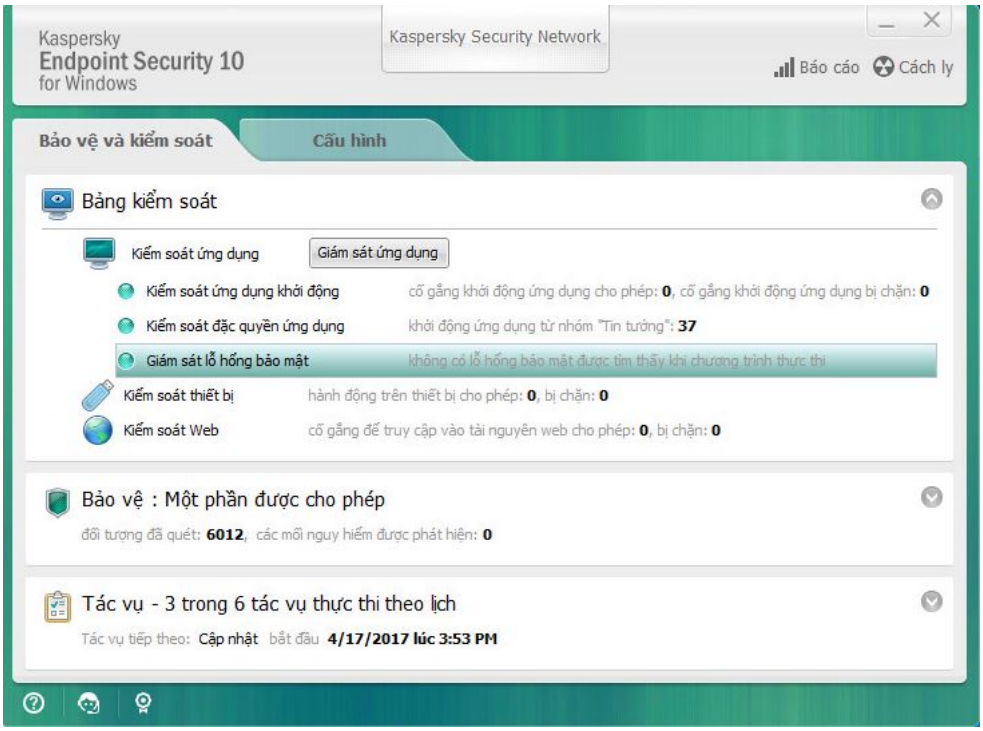
Thẻ Bảo vệ và Kiểm soát Ứng dụng

Thẻ Bảo vệ và Kiểm soát của Kaspersky Endpoint Security nhằm cung cấp thông tin chung về hiệu năng của tất cả các tác vụ và hoạt động của tất cả các thành phần ứng dụng. Trên thẻ này, bạn cũng có thể quản lý hoạt động của các thành phần và hiệu năng của các tác vụ.

Thẻ Bảo vệ và Kiểm soát Ứng dụng gồm ba gồm (xem hình dưới đây):

- Mục **Bảng kiểm soát** chứa một danh sách các thành phần kiểm soát.
- Mục **Quản lý tính năng bảo vệ** chứa một danh sách các thành phần bảo vệ Chống virus.
- Mục **Tác vụ** chứa một danh sách các tác vụ cục bộ được chạy trên máy tính.

Mỗi mục đều chứa các yếu tố kiểm soát mà bạn có thể sử dụng để bật hoặc tắt hoạt động của một thành phần, truy cập cấu hình của thành phần hoặc tác vụ được chọn, và xem số liệu hoạt động của thành phần hoặc tác vụ được chọn.



Thẻ Bảo vệ và Kiểm soát Ứng dụng

Để mở thẻ Bảo vệ và Kiểm soát Ứng dụng, thực hiện một trong các thao tác sau:

- Trong cửa sổ chính của ứng dụng, chọn thẻ **Bảo vệ và Kiểm soát**.
- Nhấn vào biểu tượng ứng dụng trong khu vực thông báo trên thanh tác vụ của Microsoft Windows.
- Chọn **Kaspersky Endpoint Security 10 for Windows** trong menu ngữ cảnh của biểu tượng ứng dụng.

Giấy phép ứng dụng

Mục này cung cấp thông tin về các khái niệm chung liên quan đến giấy phép sử dụng ứng dụng.

Thông tin về Thỏa thuận giấy phép người dùng cuối

Thỏa thuận giấy phép người dùng cuối là một thỏa thuận pháp lý kí kết giữa bạn và AO Kaspersky Lab, quy định các điều khoản sử dụng ứng dụng.

Hãy đọc kỹ các điều khoản của Thỏa thuận Giấy phép trước khi sử dụng ứng dụng.

Bạn có thể xem các điều khoản của Thỏa thuận Giấy phép bằng các cách sau:

- Khi cài đặt Kaspersky Endpoint Security trong chế độ tương tác.
- Bằng cách đọc tập tin license.txt. Tài liệu này được bao gồm trong gói phân phối ứng dụng.

Bằng cách xác nhận rằng bạn đồng ý với Thỏa thuận giấy phép người dùng cuối khi cài đặt ứng dụng, bạn thể hiện sự chấp nhận đối với các điều khoản của Thỏa thuận giấy phép người dùng cuối. Nếu bạn không đồng ý với các điều khoản của Thỏa thuận giấy phép người dùng cuối, bạn phải hủy bỏ việc cài đặt.

Thông tin về giấy phép

Một *giấy phép* là quyền sử dụng ứng dụng có giới hạn thời gian, được cấp theo Thỏa thuận giấy phép người dùng cuối.

Một giấy phép hợp lệ cho phép bạn hưởng các dịch vụ sau:

- Sử dụng ứng dụng tuân theo các điều khoản của Thỏa thuận giấy phép người dùng cuối
- Hỗ trợ kỹ thuật

Phạm vi của dịch vụ và điều khoản sử dụng ứng dụng tùy thuộc vào kiểu giấy phép theo đó mà ứng dụng đã được kích hoạt.

Các kiểu giấy phép sau được cung cấp:

- *Dùng thử* – một giấy phép miễn phí có mục đích để dùng thử ứng dụng.

  Giấy phép dùng thử thường có một thời hạn ngắn. Khi giấy phép dùng thử hết hạn, tất cả các tính năng của Kaspersky Endpoint Security sẽ bị tắt. Để tiếp tục sử dụng ứng dụng, bạn cần mua một giấy phép thương mại.

  Bạn chỉ có thể kích hoạt ứng dụng theo giấy phép dùng thử một lần duy nhất.

- *Thương mại* – một giấy phép có phí được cung cấp khi bạn mua Kaspersky Endpoint Security.

  Chức năng ứng dụng được cung cấp theo giấy phép thương mại tùy thuộc vào loại sản phẩm. Sản phẩm được chọn được ghi trong Chứng chỉ giấy phép. Thông tin về các sản phẩm khả dụng có thể được tìm thấy trên trang web Kaspersky.

Khi giấy phép thương mại hết hạn, các tính năng chính của ứng dụng sẽ bị vô hiệu. Để tiếp tục sử dụng ứng dụng, bạn phải gia hạn giấy phép thương mại của mình. Nếu bạn không định gia hạn giấy phép, bạn phải gỡ bỏ ứng dụng khỏi máy tính của mình.

Thông tin về chứng nhận giấy phép

Chứng nhận giấy phép là một tài liệu được chuyển đến người dùng cùng với tập tin khóa hoặc mã kích hoạt.

Chứng nhận giấy phép chứa các thông tin giấy phép sau:

- Số đơn hàng
- Chi tiết của người dùng được cấp giấy phép
- Chi tiết của ứng dụng có thể được kích hoạt sử dụng giấy phép
- Giới hạn về số đơn vị được cấp phép (ví dụ, số thiết bị có thể sử dụng ứng dụng theo giấy phép)
- Ngày bắt đầu thời hạn giấy phép
- Ngày hết hạn giấy phép hoặc thời hạn giấy phép
- Loại giấy phép

Thông tin về gói đăng ký

Gói đăng ký cho Kaspersky Endpoint Security là một đơn hàng cho ứng dụng với các tham số cụ thể (thời hạn kết thúc gói đăng ký, số thiết bị được bảo vệ). Bạn có thể đặt gói đăng ký cho Kaspersky Endpoint Security từ nhà cung cấp dịch vụ của bạn (ví dụ như ISP). Một gói đăng ký có thể được gia hạn thủ công hoặc tự động, hoặc bạn có thể hủy bỏ gói đăng ký. Bạn có thể quản lý gói đăng ký trên website của nhà cung cấp dịch vụ.

Gói đăng ký có thể có giới hạn (ví dụ như trong một năm) hoặc không giới hạn (không có ngày hết hạn). Để ứng dụng Kaspersky Endpoint Security có thể tiếp tục hoạt động sau khi kết thúc thời hạn đăng ký có giới hạn, bạn phải gia hạn gói đăng ký của mình. Gói đăng ký không giới hạn sẽ tự động được gia hạn nếu dịch vụ của nhà cung cấp đã được trả trước đúng hạn.

Trong trường hợp gói đăng ký là có giới hạn, khi gói đăng ký này hết hạn, bạn có thể sẽ được tặng một thời gian ân hạn để gia hạn gói đăng ký của mình, trong thời gian này ứng dụng vẫn sẽ duy trì các chức năng của nó. Nhà cung cấp dịch vụ sẽ quyết định có nên cấp thời gian ân hạn hay không, và nếu có, xác định khoảng thời gian ân hạn.

Để sử dụng ứng dụng Kaspersky Endpoint Security theo gói đăng ký, bạn phải áp dụng mã kích hoạt nhận được từ nhà cung cấp dịch vụ. Sau khi mã kích hoạt đã được áp dụng, khóa kích hoạt sẽ được cài đặt. Khóa kích hoạt quy định giấy phép để sử dụng ứng dụng theo gói đăng ký. Một khóa bổ sung chỉ có thể được cài đặt sử dụng một mã kích hoạt và không thể được cài đặt sử dụng một tập tin khóa hoặc theo gói đăng ký.

Chức năng của ứng dụng được cung cấp theo gói đăng ký có thể tương ứng với chức năng ứng dụng cho các loại giấy phép thương mại sau: Tiêu chuẩn, Kaspersky Business Space Security, Kaspersky Enterprise Space Security. Các loại giấy phép này được thiết kế để bảo vệ máy chủ tập tin, máy trạm và thiết bị di động, và hỗ trợ việc sử dụng các thành phần kiểm soát trên máy trạm và thiết bị di động.

Các tùy chọn quản lý gói đăng ký được cung cấp có thể thay đổi tùy theo nhà cung cấp dịch vụ. Nhà cung cấp dịch vụ có thể sẽ không cấp thời gian ân hạn để gia hạn gói đăng ký, trong thời gian này ứng dụng vẫn sẽ duy trì các chức năng của nó.

Mã kích hoạt được mua theo gói đăng ký có thể sẽ không được sử dụng để kích hoạt các phiên bản trước đây của Kaspersky Endpoint Security.

Thông tin về mã kích hoạt

Mã kích hoạt là một chuỗi chữ số đặc trưng gồm 20 ký tự Latinh và số mà bạn nhận được khi mua một giấy phép thương mại cho Kaspersky Endpoint Security.

Để kích hoạt ứng dụng với một mã kích hoạt, bạn cần kết nối Internet để truy cập đến các máy chủ kích hoạt của Kaspersky.

Khi ứng dụng được kích hoạt với một mã kích hoạt, khóa kích hoạt sẽ được cài đặt. Một khóa bổ sung chỉ có thể được cài đặt sử dụng một mã kích hoạt và không thể được cài đặt sử dụng một tập tin khóa hoặc theo gói đăng ký.

Nếu một mã kích hoạt bị mất sau khi kích hoạt ứng dụng, bạn có thể khôi phục lại mã kích hoạt đó. Bạn có thể cần một mã kích hoạt, chẳng hạn, để đăng ký một tài khoản Kaspersky CompanyAccount. Để khôi phục một mã kích hoạt, bạn phải liên hệ với bộ phận Hỗ trợ kỹ thuật của Kaspersky.

Thông tin về chìa khóa

Một *khóa* là một chuỗi chữ số đặc trưng. Một khóa cho phép bạn sử dụng ứng dụng theo điều khoản được quy định trong Chứng nhận Giấy phép (loại giấy phép, thời gian hiệu lực của giấy phép, hạn chế giấy phép).

Một chứng nhận giấy phép sẽ không được cung cấp cho khóa được cài đặt theo diện gói đăng ký

Một khóa có thể được bổ sung vào ứng dụng với một mã kích hoạt hoặc tập tin khóa.

Bạn có thể thêm, sửa hoặc xóa khóa. Key có thể bị chặn bởi Kaspersky nếu các điều khoản của Thỏa thuận giấy phép người dùng cuối bị vi phạm. Nếu một khóa đã bị đưa vào danh sách đen, bạn sẽ phải bổ sung một khóa khác để có thể tiếp tục sử dụng ứng dụng.

Nếu một khóa cho một giấy phép hết hạn đã bị xóa, chức năng ứng dụng sẽ không được cung cấp. Bạn không thể bổ sung lại khóa đó sau khi nó đã bị xóa.

Có hai loại khóa: kích hoạt và bổ sung.

Key kích hoạt là một khóa hiện đang được sử dụng bởi ứng dụng. Một khóa giấy phép thương mại hoặc dùng thử có thể được thêm làm khóa kích hoạt. Ứng dụng không thể có nhiều hơn một khóa kích hoạt.

Một *khóa bổ sung* là khóa chứng nhận quyền sử dụng ứng dụng của người dùng, nhưng hiện không được sử dụng. Khi khóa kích hoạt hết hạn sử dụng, một khóa bổ sung sẽ tự động được kích hoạt. Một khóa bổ sung chỉ có thể được thêm vào khi đã có khóa kích hoạt.

Một khóa cho giấy phép dùng thử chỉ có thể được thêm làm khóa kích hoạt. Nó không thể được thêm dưới dạng khóa bổ sung. Một khóa cho giấy phép dùng thử không thể thay thế khóa kích hoạt của một giấy phép thương mại.

Nếu một khóa bị cho vào danh sách đen, chức năng của ứng dụng được quy định bởi giấy phép mà theo đó ứng dụng được kích hoạt vẫn sẽ được cung cấp trong 8 ngày. Kaspersky Security Network cùng các bản cập nhật cơ sở dữ liệu và mô-đun ứng dụng vẫn sẽ được cung cấp mà không có giới hạn. Ứng dụng sẽ thông báo với người dùng rằng khóa đã bị cho vào danh sách đen. Sau 8 ngày, chức năng của ứng dụng sẽ bị giới hạn đến cấp độ chức năng được cung cấp sau khi thời hạn giấy phép đã kết thúc: ứng dụng sẽ hoạt động mà không có các bản cập nhật, và Kaspersky Security Network sẽ không thể được sử dụng.

Thông tin về tập tin khóa

Một *tập tin key* là một tập tin có phần mở rộng .key mà bạn nhận được từ Kaspersky sau khi mua Kaspersky Endpoint Security. Mục đích của tập tin khóa là để thêm một khóa kích hoạt ứng dụng.

Bạn không cần phải kết nối đến các máy chủ kích hoạt của Kaspersky để kích hoạt ứng dụng với một tập tin key.

Bạn có thể khôi phục một tập tin khóa nếu nó đã bị xóa nhầm. Bạn có thể cần một tập tin khóa, chẳng hạn, để đăng ký một tài khoản Kaspersky CompanyAccount.

Để khôi phục một tập tin khóa, hãy thực hiện một trong các thao tác sau:

- Liên hệ với nhà cung cấp giấy phép.
- Nhận tập tin key trên Website Kaspersky dựa trên mã kích hoạt hiện có của bạn.

Khi ứng dụng được kích hoạt bằng một tập tin khóa, một khóa hiện hoạt sẽ được thêm. Bạn chỉ có thể thêm khóa giấy phép dự trữ bằng cách sử dụng tập tin khóa và bạn không thể thêm bằng cách sử dụng mã kích hoạt.

Thông tin về cung cấp dữ liệu

Bằng cách chấp nhận Thỏa thuận Giấy phép Người dùng Cuối, bạn đồng ý tự động truyền tải thông tin về việc sử dụng sản phẩm của mình, cũng như kiểu, phiên bản và ngôn ngữ bản địa của chương trình được cài đặt, các định danh riêng của trình cài đặt chương trình và kiểu cài đặt, và dữ liệu về các khóa hoạt động và khóa bổ sung (bao gồm kiểu giấy phép, thời hạn hiệu lực, ngày kích hoạt chương trình và ngày hết hạn giấy phép, và số hiệu của giấy phép, trạng thái hiện tại của giấy phép, phiên bản của giao thức tương tác với máy chủ kích hoạt).

Nếu chương trình được kích hoạt với một mã kích hoạt, để nhận thông tin thống kê về việc phân phối và sử dụng sản phẩm của Chủ Sở hữu Giấy phép, bạn đồng ý tự động cung cấp phiên bản của chương trình đang được sử dụng (bao gồm thông tin về các bản cập nhật chương trình đã được cài đặt, định danh cài đặt chương trình, thông tin về giấy phép), phiên bản của hệ điều hành, và các định danh thành phần của chương trình đang hoạt động tại thời điểm thông tin được cung cấp.

Thông tin được nhận sẽ được bảo vệ bởi Kaspersky Lab theo luật pháp, các yêu cầu và quy định hiện hành của Kaspersky.

Kaspersky sẽ sử dụng thông tin được nhận một cách hoàn toàn ẩn danh và chỉ dưới dạng dữ liệu thống kê chung. Số liệu thống kê nói chung được tự động tạo sử dụng các thông tin được thu thập ban đầu và không chứa bất kỳ dữ liệu cá nhân hay thông tin bí mật nào khác. Thông tin được thu thập ban đầu sẽ được tiêu hủy khi được tích lũy (mỗi năm một lần). Dữ liệu thống kê chung sẽ được lưu trữ mãi mãi.

Đọc Thỏa thuận Giấy phép Người dùng Cuối và truy cập website Kaspersky để tìm hiểu thêm về cách chúng tôi thu thập, xử lý, lưu trữ và tiêu hủy thông tin về việc sử dụng ứng dụng sau khi bạn chấp nhận Thỏa thuận Giấy phép Người dùng Cuối và đồng ý với Tuyên bố KSN. Các tập tin license.txt và ksn.txt chứa Thỏa thuận Giấy phép Người dùng Cuối và Tuyên bố KSN và là một phần của gói phân phối của chương trình.

Xem thông tin giấy phép

Để xem thông tin giấy phép:

1. Mở cửa sổ chính của ứng dụng.
2. Nhấn vào nút / ở phần dưới của cửa sổ chính của ứng dụng.

   Cửa sổ **Bản quyền** sẽ được mở ra. Thông tin về giấy phép được hiển thị trong mục nằm ở phần trên của cửa sổ **Giấy phép**.

Mua giấy phép

Bạn có thể mua một giấy phép sau khi cài đặt ứng dụng. Khi mua giấy phép, bạn sẽ nhận được một mã kích hoạt hoặc tập tin khóa để kích hoạt ứng dụng.

Để mua giấy phép:

1. Mở cửa sổ chính của ứng dụng.
2. Nhấn vào nút / ở phần dưới của cửa sổ chính của ứng dụng.

   Cửa sổ **Bản quyền** sẽ được mở ra.
3. Trong cửa sổ **Bản quyền**, thực hiện một trong các thao tác sau:

   - Nếu không có khóa nào được bổ sung hoặc một khóa cho giấy phép dùng thử đã được bổ sung, nhấn nút **Đặt mua bản quyền**.
   - Nếu một khóa cho giấy phép thương mại đã được bổ sung, nhấn nút **gia hạn bản quyền**.

   Một cửa sổ sẽ được mở ra với website cửa hàng trực tuyến của Kaspersky, ở đó bạn có thể mua một giấy phép.

Gia hạn giấy phép

Khi giấy phép của bạn sắp hết hạn, bạn có thể gia hạn cho nó. Điều này đảm bảo máy tính của bạn luôn được bảo vệ sau khi hết hạn giấy phép hiện tại và cho đến khi bạn kích hoạt ứng dụng theo một giấy phép mới.

Để gia hạn giấy phép:

1. Nhận một mã kích hoạt hoặc tập tin khóa mới cho ứng dụng.
2. Thêm một khóa bổ sung với mã kích hoạt hoặc tập tin khóa mà bạn vừa nhận.

   Một khóa bổ sung sẽ được thêm. Nó sẽ trở thành kích hoạt khi giấy phép hết hạn.

Có thể sẽ mất một thời gian để khóa được cập nhật từ trạng thái bổ sung sang kích hoạt do phân phối tải giữa các máy chủ kích hoạt của Kaspersky.

Gia hạn gói đăng ký

Khi bạn sử dụng ứng dụng theo gói đăng ký, Kaspersky Endpoint Security sẽ tự động liên hệ với máy chủ kích hoạt theo các chu kỳ cụ thể cho đến khi gói đăng ký của bạn đã hết hạn.

Nếu bạn sử dụng ứng dụng theo gói đăng ký không giới hạn, Kaspersky Endpoint Security sẽ tự động kiểm tra với máy chủ kích hoạt cho các khóa được gia hạn trong chế độ nền. Nếu một khóa là khả dụng trên máy chủ kích hoạt, ứng dụng sẽ bổ sung nó bằng cách thay thế khóa cũ. Bằng cách này, gói đăng ký không giới hạn của Kaspersky Endpoint Security sẽ được gia hạn mà không cần người dùng xử lý.

Nếu bạn sử dụng ứng dụng theo gói đăng ký giới hạn, vào ngày gói đăng ký (hoặc thời gian ân hạn sau khi gói đăng ký hết hạn, trong thời gian đó việc gia hạn gói đăng ký có thể được thực hiện) hết hạn, Kaspersky Endpoint Security sẽ hiển thị một thông báo tương ứng và dừng nỗ lực gia hạn gói đăng ký một cách tự động. Trong trường hợp này, Kaspersky Endpoint Security sẽ hành xử như khi một giấy phép thương mại cho ứng dụng bị hết hạn: ứng dụng sẽ hoạt động mà không có bản cập nhật, và Kaspersky Security Network sẽ không thể được sử dụng.

Bạn có thể gia hạn gói đăng ký trên website của nhà cung cấp dịch vụ.

Bạn có thể cập nhật trạng thái gói đăng ký một cách thủ công trong cửa sổ **Bản quyền**. Việc này có thể là cần thiết nếu gói đăng ký đã được gia hạn sau khi kết thúc thời gian ân hạn và ứng dụng đã không tự động cập nhật trạng thái gói đăng ký.

Truy cập website của nhà cung cấp dịch vụ

Để truy cập website của nhà cung cấp dịch vụ từ giao diện ứng dụng:

1. Mở cửa sổ chính của ứng dụng.
2. Nhấn vào nút / ở phần dưới của cửa sổ chính của ứng dụng.

Cửa sổ **Bản quyền** sẽ được mở ra.

3. Trong cửa sổ **Bản quyền**, nhấn **Liên hệ với nhà cung cấp**.

Thông tin về các phương thức kích hoạt ứng dụng

Kích hoạt là quy trình kích hoạt một giấy phép cho phép bạn sử dụng phiên bản đầy đủ chức năng của ứng dụng cho đến khi giấy phép hết hạn. Quy trình kích hoạt ứng dụng liên quan đến việc bổ sung thêm khóa.

Bạn có thể kích hoạt ứng dụng theo một trong những cách sau đây:

- Khi cài đặt ứng dụng, với sự trợ giúp của Trình hướng dẫn Thiết lập Ban đầu. Bạn có thể thêm khóa kích hoạt bằng cách này.
- Nội bộ từ giao diện ứng dụng, bằng cách sử dụng Trình hướng dẫn Kích hoạt. Bạn có thể thêm cả khóa kích hoạt và khóa bổ sung bằng cách này.
- Từ xa với bộ phần mềm Kaspersky Security Center bằng cách tạo, sau đó bắt đầu một tác vụ thêm khóa. Bạn có thể thêm cả khóa kích hoạt và khóa bổ sung bằng cách này.
- Từ xa bằng cách phân phối khóa và mã kích hoạt được lưu trữ trong kho lưu trữ khóa của Máy chủ Quản trị của Kaspersky Security Center đến các máy khách (xem *Hướng dẫn dành cho Quản trị viên Kaspersky Security Center* để biết thêm chi tiết). Bạn có thể thêm cả khóa kích hoạt và khóa bổ sung bằng cách này.

  Mã kích hoạt được mua theo gói đăng ký sẽ được phân phối đầu tiên.

- Sử dụng dòng lệnh.

Có thể sẽ mất một thời gian để ứng dụng được kích hoạt với một mã kích hoạt (trong quá trình cài đặt từ xa hoặc phi tương tác) do phân phối tải giữa các máy chủ kích hoạt của Kaspersky. Nếu bạn cần kích hoạt ứng dụng ngay lập tức, bạn có thể ngắt tiến trình kích hoạt đang diễn ra và bắt đầu kích hoạt sử dụng Trình hướng dẫn Kích hoạt.

Sử dụng Trình hướng dẫn Kích hoạt để kích hoạt ứng dụng

Để kích hoạt Kaspersky Endpoint Security bằng cách sử dụng Trình hướng dẫn Kích hoạt:

1. Nhấn vào nút / ở phần dưới của cửa sổ chính của ứng dụng.
   Cửa sổ **Bản quyền** sẽ được mở ra.
2. Trong cửa sổ **Bản quyền**, nhấn nút **Kích hoạt ứng dụng theo một giấy phép mới**.
   Trình hướng dẫn Kích hoạt Ứng dụng sẽ được bắt đầu.
3. Làm theo chỉ dẫn của Trình hướng dẫn Kích hoạt.

Để biết thêm chi tiết về thủ tục kích hoạt ứng dụng, vui lòng xem mục này trên Trình hướng dẫn Thiết lập Ban đầu.

Kích hoạt ứng dụng từ dòng lệnh

Để kích hoạt ứng dụng từ dòng lệnh,

nhập `avp.com license /add <mã kích hoạt hoặc tập tin khóa> /password=<mật khẩu>` trong dòng lệnh.

Khởi chạy và dừng ứng dụng

Mục này mô tả cách bạn có thể thiết lập khởi động tự động ứng dụng, bắt đầu hoặc dừng ứng dụng một cách thủ công, và tạm ngưng hoặc khôi phục các thành phần bảo vệ và kiểm soát.

Bật và tắt tính năng tự động khởi chạy ứng dụng

Tự động khởi chạy có nghĩa là Kaspersky Endpoint Security sẽ được khởi chạy ngay sau khi khởi động hệ điều hành, mà không cần người dùng can thiệp. Tính năng khởi chạy tự động ứng dụng được bật theo mặc định.

Sau khi cài đặt, Kaspersky Endpoint Security sẽ được khởi chạy tự động lần đầu tiên. Sau đó, ứng dụng sẽ được khởi chạy tự động sau mỗi lần khởi động hệ điều hành.

Việc tải về cơ sở dữ liệu chống virus của Kaspersky Endpoint Security sau khi hệ điều hành được khởi động có thể tốn đến hai phút tùy thuộc vào công suất máy tính. Trong thời gian này, cấp độ bảo vệ máy tính sẽ bị giảm sút. Việc tải về cơ sở dữ liệu chống virus khi Kaspersky Endpoint Security được khởi chạy trên một hệ điều hành đã được nạp đầy đủ sẽ không gây suy giảm cấp độ bảo vệ máy tính.

Để bật và tắt tính năng tự động khởi chạy ứng dụng:

1. Mở cửa sổ cấu hình ứng dụng.
2. Chọn mục **Bảo vệ Chống virus** ở phía bên trái.
   Cấu hình bảo vệ chống virus sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Thực hiện một trong các thao tác sau:
   - Nếu bạn muốn bật chế độ tự động thực thi ứng dụng, chọn hộp kiểm **Bắt đầu Kaspersky Endpoint Security 10 for Windows khi khởi động máy tính**.
   - Nếu bạn muốn tắt chế độ tự động thực thi ứng dụng, xóa hộp kiểm **Bắt đầu Kaspersky Endpoint Security 10 for Windows khi khởi động máy tính**.
4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Khởi chạy và dừng ứng dụng một cách thủ công

Các chuyên gia Kaspersky khuyên bạn không nên dừng thủ công Kaspersky Endpoint Security bởi điều này sẽ khiến máy tính và dữ liệu cá nhân của bạn bị đe dọa. Nếu cần, bạn có thể tạm ngưng bảo vệ máy tính trong thời gian cần thiết mà không dừng hẳn ứng dụng.

Kaspersky Endpoint Security cần được khởi chạy thủ công nếu trước đó bạn đã tắt tự động khởi chạy cho ứng dụng.

Để khởi chạy ứng dụng một cách thủ công,

Trong menu **Start**, chọn **Applications** → **Kaspersky Endpoint Security 10 for Windows**.

Để dừng ứng dụng một cách thủ công:

1. Nhấn phải chuột để gọi menu ngữ cảnh của biểu tượng ứng dụng trong khu vực thông báo trên thanh tác vụ.
2. Trong menu ngữ cảnh, chọn **Thoát**.

Tạm ngưng và khôi phục tính năng bảo vệ và kiểm soát máy tính

Tạm ngưng bảo vệ và kiểm soát máy tính có nghĩa là tắt tất cả các thành phần bảo vệ và kiểm soát của Kaspersky Endpoint Security trong một thời gian nhất định.

Trạng thái ứng dụng sẽ được hiển thị qua biểu tượng ứng dụng trong khu vực thông báo trên thanh tác vụ.

- Biểu tượng thể hiện rằng tính năng bảo vệ và kiểm soát máy tính đang bị tạm ngưng.
- Biểu tượng thể hiện rằng tính năng bảo vệ và kiểm soát máy tính đang bị tắt.

Việc tạm ngưng và khôi phục tính năng bảo vệ và kiểm soát máy tính không ảnh hưởng đến các tác vụ quét hoặc cập nhật.

Nếu có bất kỳ kết nối mạng nào đã được thiết lập khi bạn tạm ngưng hoặc khôi phục tính năng bảo vệ và kiểm soát máy tính, một thông báo về việc chấm dứt các kết nối mạng này sẽ được hiển thị.

Để tạm ngưng bảo vệ và kiểm soát máy tính:

1. Nhấn phải chuột để gọi menu ngữ cảnh của biểu tượng ứng dụng trong khu vực thông báo trên thanh tác vụ.
2. Trong menu ngữ cảnh, chọn **Tạm ngưng bảo vệ và kiểm soát**.

   Cửa sổ **Tạm dừng bảo vệ** sẽ được mở ra.
3. Chọn một trong các tùy chọn sau:
   - **Tạm dừng theo thời gian chỉ định** - Tính năng bảo vệ và kiểm soát máy tính sẽ được khôi phục sau khoảng thời gian được quy định trong danh sách thả xuống bên dưới.
   - **Tạm dừng cho đến khi khởi động lại**- Tính năng bảo vệ và kiểm soát máy tính sẽ được khôi phục sau khi bạn thoát và mở lại ứng dụng, hoặc khởi động lại hệ điều hành. Tính năng tự động khởi chạy ứng dụng phải được bật để sử dụng tùy chọn này.
   - **Tạm dừng** - Tính năng bảo vệ và kiểm soát máy tính sẽ được khôi phục khi bạn quyết định bật lại chúng.
4. Nếu bạn đã chọn mục **Tạm dừng theo thời gian chỉ định** ở bước trước đó, hãy chọn khoảng thời gian cần thiết trong danh sách thả xuống.

Để khôi phục lại bảo vệ và kiểm soát máy tính:

1. Nhấn phải chuột để gọi menu ngữ cảnh của biểu tượng ứng dụng trong khu vực thông báo trên thanh tác vụ.

2. Trong menu ngữ cảnh, chọn **Khôi phục bảo vệ và kiểm soát**.

Bạn có thể khôi phục tính năng bảo vệ và kiểm soát máy tính bất cứ lúc nào, bất kể tùy chọn tạm ngưng bảo vệ và kiểm soát máy tính mà bạn đã chọn trước đó.

Bảo vệ hệ thống tập tin trên máy tính. Chống virus cho tập tin

Mục này chứa thông tin về Chống virus cho tập tin và chỉ dẫn cách để thiết lập cấu hình thành phần.

Thông tin về Chống virus cho tập tin

Chống Virus cho Tập tin bảo vệ hệ thống tập tin của máy tính khỏi bị nhiễm virus. Theo mặc định, Chống virus cho tập tin sẽ khởi động cùng với Kaspersky Endpoint Security, liên tục hoạt động trong bộ nhớ máy tính và quét tất cả các tập tin được mở ra, lưu lại hoặc khởi động trên máy tính và trên tất cả các ổ đĩa được kết nối với nó để phát hiện virus và các mối đe dọa khác.

Khi phát hiện một mối đe dọa trong một tập tin, Kaspersky Endpoint Security sẽ thực hiện hành động sau:

1. Xác định loại đối tượng được phát hiện trong tập tin (ví dụ như *virus* hoặc *trojan*).
2. Dán nhãn cho tập tin đó là *có khả năng bị nhiễm* nếu tác vụ quét không thể xác định liệu tập tin đó bị nhiễm hay không. Tập tin có thể chứa một chuỗi mã giống với một virus hoặc phần mềm độc hại khác, hoặc một bản sửa đổi của một virus đã biết.
3. Ứng dụng sẽ hiển thị một thông báo về đối tượng độc hại được phát hiện trong tập tin (nếu các thông báo được thiết lập), và xử lý tập tin đó bằng cách thực hiện hành động được quy định trong cấu hình Chống virus cho tập tin.

Bật và tắt Chống virus cho tập tin

Theo mặc định, Chống virus cho tập tin sẽ được bật và chạy trong một chế độ được khuyến nghị bởi các chuyên gia của Kaspersky. Bạn có thể tắt Chống virus cho tập tin nếu cần thiết.

Có hai cách để bật hoặc tắt thành phần này:

- Trên thẻ **Bảo vệ và Kiểm soát** của cửa sổ chính của ứng dụng
- Từ cửa sổ cấu hình ứng dụng.

Để bật hoặc tắt Chống virus cho tập tin trên thẻ Bảo vệ và Kiểm soát của cửa sổ chính của ứng dụng:

1. Mở cửa sổ chính của ứng dụng.
2. Chọn thẻ **Bảo vệ và Kiểm soát**.
3. Nhấn vào mục **Bảo vệ**.

   Mục **Bảo vệ** sẽ được mở ra.
4. Nhấn phải chuột để gọi menu ngữ cảnh của dòng có chứa thông tin về thành phần Chống virus cho tập tin.

   Một menu để chọn hành động đối với thành phần sẽ được mở ra.
5. Thực hiện một trong các thao tác sau:

- Để bật Chống virus cho tập tin, chọn **Bắt đầu** trong menu.

  Biểu tượng trạng thái của thành phần , được hiển thị ở bên trái của dòng **Chống virus cho tập tin** sẽ được chuyển sang biểu tượng .

- Để tắt Chống virus cho tập tin, chọn **Dừng** trong menu.

  Biểu tượng trạng thái của thành phần , được hiển thị ở bên trái của dòng **Chống virus cho tập tin** sẽ được chuyển sang biểu tượng .

Để bật hoặc tắt Chống virus cho tập tin từ cửa sổ cấu hình ứng dụng:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Chống virus cho tập tin**.

   Ở phần bên phải của cửa sổ, cấu hình của thành phần Chống virus cho tập tin sẽ được hiển thị.
3. Thực hiện một trong các thao tác sau:

   - Nếu bạn muốn bật Chống virus cho tập tin, chọn hộp kiểm **Bật Chống Virus cho Tập tin**.
   - Nếu bạn muốn tắt Chống virus cho tập tin, xóa hộp kiểm **Bật Chống Virus cho Tập tin**.
4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Tự động tạm ngưng Chống virus cho tập tin

Bạn có thể thiết lập Chống virus cho tập tin để tự động tạm ngưng tại một thời điểm cụ thể, hoặc khi xử lý các chương trình cụ thể.

Tạm ngưng Chống virus cho tập tin khi nó xung đột với một số chương trình là một biện pháp khẩn cấp. Trong trường hợp xảy ra xung đột trong quá trình hoạt động của một thành phần, chúng tôi khuyến nghị bạn liên hệ với Hỗ trợ kỹ thuật của Kaspersky (https://companyaccount.kaspersky.com). Các chuyên gia hỗ trợ sẽ giúp bạn thiết lập Chống virus cho tập tin để chạy cùng với các chương trình khác trên máy tính của bạn.

Để thiết lập tự động tạm ngưng Chống virus cho tập tin:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Chống virus cho tập tin**.

   Ở phần bên phải của cửa sổ, cấu hình của thành phần Chống virus cho tập tin sẽ được hiển thị.
3. Trong mục **Mức độ bảo mật**, nhấn nút **Cấu hình**.

   Cửa sổ **Chống virus cho tập tin** sẽ được mở ra.
4. Trong cửa sổ **Chống virus cho tập tin**, chọn thẻ **Bổ sung**.
5. Trong mục **Tạm dừng tác vụ**:

- Để thiết lập tự động tạm ngưng Chống virus cho tập tin tại một thời điểm cụ thể, chọn hộp kiểm **Theo lập lịch** và nhấn nút **Lập lịch**.

  Cửa sổ **Tạm dừng tác vụ** sẽ được mở ra.

- Để thiết lập tự động tạm ngưng Chống virus cho tập tin khi khởi chạy các ứng dụng cụ thể, chọn hộp kiểm **Lúc ứng dụng khởi động** và nhấn nút **Lựa chọn**.

  Cửa sổ **Ứng dụng** sẽ được mở ra.

6. Thực hiện một trong các thao tác sau:

   - Nếu bạn đang thiết lập tự động tạm ngưng Chống virus cho tập tin tại một thời điểm cụ thể, trong cửa sổ **Tạm dừng tác vụ**, sử dụng các trường **Tác vụ tạm dừng lúc** và **Khôi phục lại tác vụ lúc** để quy định khoảng thời gian (theo định dạng HH:MM) trong đó Chống virus cho tập tin được tạm ngưng. Nhấn **OK**.

   - Nếu bạn đang thiết lập tự động tạm ngưng Chống virus cho tập tin khi khởi chạy các ứng dụng cụ thể, sử dụng các nút **Thêm**, **Chỉnh sửa** và **Gỡ bỏ** trong cửa sổ **Ứng dụng** để tạo một danh sách các ứng dụng mà trong thời gian hoạt động của chúng, Chống virus cho tập tin sẽ bị tạm ngưng. Nhấn **OK**.

7. Trong cửa sổ **Chống virus cho tập tin**, nhấn **OK**.

8. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Thiết lập Chống virus cho tập tin

Bạn có thể làm như sau để thiết lập cho Chống virus cho tập tin:

- Thay đổi cấp độ bảo mật.

  Bạn có thể chọn một trong các cấp độ bảo mật được thiết lập sẵn hoặc tự cấu hình thiết lập cấp độ bảo mật. Nếu bạn đã thay đổi thiết lập cấp độ bảo mật, bạn luôn có thể quay lại thiết lập cấp độ bảo mật được khuyến nghị.

- Thay đổi hành động được thực hiện bởi Chống virus cho tập tin khi phát hiện một tập tin bị nhiễm.

- Sửa phạm vi bảo vệ của Chống virus cho tập tin.

  Bạn có thể mở rộng hoặc hạn chế phạm vi bảo vệ bằng cách thêm hoặc xóa các đối tượng quét, hoặc bằng cách thay đổi loại tập tin được quét.

- Thiết lập Trình phân tích suy nghiệm.

  Chống virus cho tập tin sử dụng một kỹ thuật được gọi là phân tích dấu hiệu. Trong quá trình phân tích dấu hiệu, Chống virus cho tập tin sẽ đối chiếu đối tượng được phát hiện với các hồ sơ trong cơ sở dữ liệu chống virus của ứng dụng. Theo khuyến nghị của các chuyên gia Kaspersky, tính năng phân tích dấu hiệu luôn được bật.

  Để tăng hiệu quả bảo vệ, bạn có thể sử dụng phân tích suy nghiệm. Trong phân tích suy nghiệm, Chống virus cho tập tin sẽ phân tích hoạt động của các đối tượng trong hệ điều hành. Phân tích suy nghiệm cho phép phát hiện các đối tượng độc hại không có hồ sơ trong cơ sở dữ liệu chống virus của ứng dụng.

- Tối ưu quét.

Bạn có thể tối ưu tốc độ quét tập tin được thực hiện bởi Chống virus cho tập tin, giảm thiểu thời gian quét và tăng tốc độ hoạt động của Kaspersky Endpoint Security. Điều này có thể có được bằng cách chỉ quét các tập tin mới và các tập tin đã được thay đổi kể từ lần quét gần nhất. Chế độ này được áp dụng cho cả các tập tin đơn và tập tin hỗn hợp.

Bạn cũng có thể bật các công nghệ iChecker và iSwift, giúp tối ưu tốc độ quét tập tin bằng cách loại trừ các tập tin chưa được sửa đổi kể từ lần quét gần nhất.

- Thiết lập quét các tập tin hỗn hợp.
- Thay đổi chế độ quét tập tin.

Thay đổi cấp độ bảo mật

Để bảo vệ hệ thống tập tin của máy tính, Chống virus cho tập tin sẽ áp dụng nhiều nhóm cấu hình khác nhau. Các nhóm thiết lập này được gọi là *cấp độ bảo mật*. Có 3 cấp độ bảo mật được thiết lập sẵn: **Cao**, **Khuyên dùng**, và **Thấp**. Cấu hình cấp độ bảo mật **Khuyên dùng** được coi là thiết lập tối ưu được khuyến nghị bởi các chuyên gia Kaspersky.

Để thay đổi một cấp độ bảo mật:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Chống virus cho tập tin**.

   Ở phần bên phải của cửa sổ, cấu hình của thành phần Chống virus cho tập tin sẽ được hiển thị.
3. Trong mục **Mức độ bảo mật**, thực hiện một trong những hành động sau:
   - Nếu bạn muốn áp dụng một trong những cấp độ bảo mật được thiết lập sẵn (**Cao**, **Khuyên dùng**, hoặc **Thấp**), hãy chọn nó với thanh trượt.
   - Nếu bạn muốn thiết lập một cấp độ bảo mật tùy chỉnh, nhấn nút **Thiết lập** và nhập thiết lập tùy chỉnh của bạn trong cửa sổ **Chống virus cho tập tin** được mở ra.

     Sau khi bạn thiết lập một cấp độ bảo mật tùy chỉnh, tên của cấp độ bảo mật trong mục **Mức độ bảo mật** sẽ được chuyển thành **Tùy chỉnh**.
   - Nếu bạn muốn thay đổi cấp độ bảo mật thành **Khuyên dùng**, nhấn nút **Mặc định**.
4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Thay đổi hành động xử lý tập tin bị nhiễm của Chống virus cho tập tin

Để thay đổi hành động xử lý tập tin bị nhiễm của Chống virus cho tập tin:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Chống virus cho tập tin**.

   Ở phần bên phải của cửa sổ, cấu hình của thành phần Chống virus cho tập tin sẽ được hiển thị.

3. Trong mục **Hành động khi phát hiện nguy hiểm**, chọn các tùy chọn cần thiết:

   - **Lựa chọn hành động tự động**.
   - **Thực hiện hành động: Khử mã độc. Xóa nếu khử mã độc không thành công**.
   - **Thực hiện hành động: Khử mã độc**.

     Nếu mục này được chọn, Kaspersky Endpoint Security sẽ áp dụng hành động **Gỡ bỏ** đến các tập tin là một phần của ứng dụng Windows Store.

   - **Thực hiện hành động: Gỡ bỏ**.
   - **Thực hiện hành động: Ngăn chặn**.

4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Sửa phạm vi bảo vệ của Chống virus cho tập tin

Phạm vi bảo vệ nói đến các đối tượng được thành phần quét khi bật. Phạm vi bảo vệ của các thành phần khác nhau có các thuộc tính khác nhau. Vị trí và kiểu tập tin được quét là các thuộc tính của phạm vi bảo vệ của Chống virus cho tập tin. Theo mặc định, Chống virus cho tập tin sẽ chỉ quét các tập tin có thể bị nhiễm được lưu trữ trên các ổ cứng, ổ đĩa mạng hoặc ổ đĩa di động.

Để tạo phạm vi bảo vệ:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Chống virus cho tập tin**.

   Ở phần bên phải của cửa sổ, cấu hình của thành phần Chống virus cho tập tin sẽ được hiển thị.

3. Trong mục **Mức độ bảo mật**, nhấn nút **Cấu hình**.

   Cửa sổ **Chống virus cho tập tin** sẽ được mở ra.

4. Trong cửa sổ **Chống virus cho tập tin**, chọn thẻ **Tổng quát**.
5. Trong mục **Loại tập tin**, quy định loại tập tin mà bạn muốn được quét bởi Chống virus cho tập tin:

   - Nếu bạn muốn quét tất cả các tập tin, chọn **Tất cả các tập tin**.
   - Nếu bạn muốn quét các tập tin có định dạng dễ bị nhiễm virus nhất, hãy chọn **Quét các tập tin theo phần định dạng**.
   - Nếu bạn muốn quét các tập tin có phần mở rộng dễ bị nhiễm virus nhất, hãy chọn **Quét các tập tin theo phần mở rộng**.

   Khi chọn loại tập tin để quét, hãy nhớ các thông tin sau:

   - Có một số định dạng tập tin (ví dụ như .txt) mà khả năng xâm nhập và kích hoạt mã độc trên đó là rất thấp. Mặt khác, cũng có những tập tin chứa hoặc có thể chứa các mã thực thi (ví dụ như .exe,

.dll và .doc). Nguy cơ xâm nhập và kích hoạt mã độc trên các tập tin này là rất cao.

- Một kẻ xâm nhập có thể gửi một virus hoặc một chương trình độc hại khác đến máy tính của bạn trong một tập tin thực thi đã được đổi tên để chứa phần mở rộng .txt. Nếu bạn chọn quét tập tin theo phần mở rộng, những tập tin này sẽ được bỏ qua bởi tác vụ quét. Nếu chọn quét tập tin theo định dạng, thì bất kể phần mở rộng là gì, Chống virus cho tập tin sẽ đều phân tích đầu mục tập tin. Phân tích này có thể xác định rằng tập tin mang định dạng .exe. Những tập tin kiểu này sẽ được quét kỹ lưỡng để tìm virus và các phần mềm độc hại khác.

6. Trong danh sách **Phạm vi bảo vệ**, thực hiện một trong các thao tác sau:

   - Nếu bạn muốn bổ sung một đối tượng mới vào phạm vi quét, nhấn nút **Thêm**.
   - Nếu bạn muốn thay đổi vị trí của một đối tượng, chọn đối tượng đó từ phạm vi quét và nhấn nút **Chỉnh sửa**.

   Cửa sổ **Lựa chọn phạm vi quét** sẽ được mở ra.

   - Nếu bạn muốn xóa một đối tượng khỏi danh sách các đối tượng được quét, chọn nó từ danh sách các đối tượng được quét và nhấn nút **Gỡ bỏ**.

     Một cửa sổ để xác nhận việc xóa sẽ được mở ra.

7. Thực hiện một trong các thao tác sau:

   - Nếu bạn muốn thêm một đối tượng mới hoặc thay đổi vị trí của một đối tượng từ danh sách các đối tượng được quét, chọn đối tượng đó trong cửa sổ **Lựa chọn phạm vi quét** và nhấn nút **Thêm**.

     Tất cả các đối tượng được chọn trong cửa sổ **Lựa chọn phạm vi quét** đều được hiển thị trong cửa sổ **Chống virus cho tập tin** trong danh sách **Phạm vi bảo vệ**.

     Nhấn **OK**.

   - Nếu bạn muốn xóa một đối tượng, nhấn nút **Có** trong cửa sổ để xác nhận xóa.

8. Nếu cần thiết, lặp lại các bước 6-7 để thêm, di chuyển hoặc xóa các đối tượng khỏi danh sách các đối tượng được quét.

9. Để loại trừ một đối tượng khỏi danh sách các đối tượng được quét, xóa hộp kiểm cạnh đối tượng đó trong danh sách **Phạm vi bảo vệ**. Tuy nhiên, đối tượng vẫn sẽ có tên trong danh sách các đối tượng được quét, mặc dù nó đã bị loại trừ khỏi tác vụ quét bởi Chống virus cho tập tin.

10. Trong cửa sổ **Chống virus cho tập tin**, nhấn **OK**.

11. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Sử dụng Trình phân tích suy nghiệm với Chống virus cho tập tin

Để thiết lập việc sử dụng Trình phân tích suy nghiệm trong hoạt động của Chống virus cho tập tin:

1. Mở cửa sổ cấu hình ứng dụng.

2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Chống virus cho tập tin**.

   Ở phần bên phải của cửa sổ, cấu hình của thành phần Chống virus cho tập tin sẽ được hiển thị.

3. Trong mục **Mức độ bảo mật**, nhấn nút **Cấu hình**.
   Cửa sổ **Chống virus cho tập tin** sẽ được mở ra.
4. Trong cửa sổ **Chống virus cho tập tin**, chọn thẻ **Hiệu suất**.
5. Trong mục **Phương thức quét**:
   - Nếu bạn muốn Chống virus cho tập tin sử dụng phân tích suy nghiệm, chọn hộp kiểm **Phân tích suy nghiệm** và sử dụng thanh trượt để đặt cấp độ phân tích suy nghiệm: **Quét nhanh**, **quét vừa**, hoặc **quét kỹ**.
   - Nếu bạn không muốn Chống virus cho tập tin sử dụng phân tích suy nghiệm, xóa hộp kiểm **Phân tích suy nghiệm**.
6. Nhấn **OK**.
7. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Sử dụng công nghệ quét trong hoạt động của Chống virus cho tập tin

Để thiết lập việc sử dụng các công nghệ quét trong hoạt động của Chống virus cho tập tin:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Chống virus cho tập tin**.
   Ở phần bên phải của cửa sổ, cấu hình của thành phần Chống virus cho tập tin sẽ được hiển thị.
3. Trong mục **Mức độ bảo mật**, nhấn nút **Cấu hình**.
   Cửa sổ **Chống virus cho tập tin** sẽ được mở ra.
4. Trong cửa sổ **Chống virus cho tập tin**, chọn thẻ **Bổ sung**.
5. Trong mục **Công nghệ quét**:
   - Chọn hộp kiểm đối diện tên của các công nghệ mà bạn muốn sử dụng trong hoạt động của Chống virus cho tập tin.
   - Xóa hộp kiểm đối diện tên của các công nghệ mà bạn không muốn sử dụng trong hoạt động của Chống virus cho tập tin.
6. Nhấn **OK**.
7. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Tối ưu quét tập tin

Để tối ưu quét tập tin:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Chống virus cho tập tin**.

   Ở phần bên phải của cửa sổ, cấu hình của thành phần Chống virus cho tập tin sẽ được hiển thị.
3. Nhấn nút **Cấu hình**.

   Cửa sổ **Chống virus cho tập tin** sẽ được mở ra.
4. Trong cửa sổ **Chống virus cho tập tin**, chọn thẻ **Hiệu suất**.
5. Trong mục **Tối ưu quét**, chọn hộp kiểm **Chỉ quét các tập tin mới hoặc có sự thay đổi**.
6. Nhấn **OK**.
7. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Quét các tập tin hỗn hợp

Một kỹ thuật phổ biến để che giấu virus và các phần mềm độc hại khác là nhúng chúng trong các tập tin tổ hợp ví dụ như tập nén hoặc cơ sở dữ liệu email. Để phát hiện virus và các phần mềm độc hại khác được ẩn giấu bằng cách này, tập tin hỗn hợp phải được giải nén, điều này có thể làm giảm tốc độ quét. Bạn có thể giới hạn nhóm tập tin hỗn hợp được quét để tăng tốc độ quét.

Phương thức sử dụng để xử lý một tập tin hỗn hợp bị nhiễm (khử nhiễm hoặc xóa) tùy thuộc vào loại tập tin.

Chống virus cho tập tin sẽ khử nhiễm các tập tin phức hợp trong định dạng RAR, ARJ, ZIP, CAB, và LHA, và xóa các tập tin trong mọi định dạng khác (ngoại trừ cơ sở dữ liệu email).

Để thiết lập quét các tập tin hỗn hợp:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Chống virus cho tập tin**.

   Ở phần bên phải của cửa sổ, cấu hình của thành phần Chống virus cho tập tin sẽ được hiển thị.
3. Trong mục **Mức độ bảo mật**, nhấn nút **Cấu hình**.

   Cửa sổ **Chống virus cho tập tin** sẽ được mở ra.
4. Trong cửa sổ **Chống virus cho tập tin**, chọn thẻ **Hiệu suất**.
5. Trong mục **Quét các tập tin hỗn hợp**, quy định loại tập tin hỗn hợp mà bạn muốn quét: tập nén, gói cài đặt, hoặc tập tin trong định dạng văn bản.
6. Để chỉ quét những tập tin hỗn hợp mới và đã được thay đổi, chọn hộp kiểm **Chỉ quét các tập tin mới hoặc có sự thay đổi**.

Chống virus cho tập tin sẽ chỉ quét các tập tin mới hoặc đã được thay đổi thuộc mọi thể loại.

7. Nhấn nút **Bổ sung**.

   Cửa sổ **Các tập tin hỗn hợp** sẽ được mở ra.

8. Trong mục **Tác vụ quét nền tảng**, thực hiện một trong những hành động sau:

   - Để ngăn Chống virus cho tập tin giải nén các tập tin hỗn hợp trong nền, xóa hộp kiểm **Giải nén các tập tin hỗn hợp trong chế độ nền**.
   - Để cho phép Chống virus cho tập tin giải nén các tập tin hỗn hợp khi quét ở trong nền, chọn hộp kiểm **Giải nén các tập tin hỗn hợp trong chế độ nền** và quy định giá trị cần thiết trong trường **Dung lượng tối thiểu của tập tin**.

9. Trong mục **Dung lượng giới hạn**, thực hiện một trong những hành động sau:

   - Để ngăn Chống Virus cho Tập tin giải nén các tập tin hỗn hợp quá lớn, chọn hộp kiểm **Không thực hiện giải nén các tập tin hỗn hợp lớn** và quy định giá trị cần thiết trong trường **Dung lượng tối đa của tập tin**. Chống virus cho tập tin sẽ không giải nén các tập tin hỗn hợp lớn hơn kích cỡ được quy định.
   - Để cho phép Chống Virus cho Tập tin giải nén các tập tin hỗn hợp lớn, xóa hộp kiểm **Không thực hiện giải nén các tập tin hỗn hợp lớn**.

     Một tập tin được coi là lớn nếu kích cỡ của nó vượt quá giá trị được quy định trong trường **Dung lượng tối đa của tập tin**.

   Chống Virus cho Tập tin sẽ quét các tập tin lớn được giải nén từ tập nén, bất kể là hộp kiểm **Không thực hiện giải nén các tập tin hỗn hợp lớn** có được chọn hay không.

10. Nhấn **OK**.

11. Trong cửa sổ **Chống virus cho tập tin**, nhấn **OK**.

12. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Thay đổi chế độ quét

Chế độ quét nghĩa là điều kiện mà theo đó Chống virus cho tập tin sẽ bắt đầu quét các tập tin. Theo mặc định, Kaspersky Endpoint Security sẽ quét các tập tin trong chế độ thông minh. Trong chế độ quét tập tin này, Chống virus cho tập tin sẽ quyết định liệu có nên quét các tập tin sau khi đã phân tích các hoạt động được thực thi với một tập tin bởi người dùng, bởi một ứng dụng thay mặt cho người dùng (với tài khoản được sử dụng để đăng nhập hoặc một tài khoản người dùng khác), hoặc bởi hệ điều hành. Ví dụ, khi làm việc với tài liệu Microsoft Office Word, Kaspersky Endpoint Security sẽ quét tập tin khi nó được mở lần đầu tiên và đóng lần cuối cùng. Các hành động tức thì ghi đè tập tin không khiến tập tin bị quét.

Để thay đổi chế độ quét tập tin:

1. Mở cửa sổ cấu hình ứng dụng.

2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Chống virus cho tập tin**.

   Ở phần bên phải của cửa sổ, cấu hình của thành phần Chống virus cho tập tin sẽ được hiển thị.

3. Trong mục **Mức độ bảo mật**, nhấn nút **Cấu hình**.
   Cửa sổ **Chống virus cho tập tin** sẽ được mở ra.
4. Trong cửa sổ **Chống virus cho tập tin**, chọn thẻ **Bổ sung**.
5. Trong mục **Chế độ quét**, chọn chế độ cần thiết:
   - **Chế độ thông minh**.
   - **Truy xuất và sửa đổi**.
   - **Theo truy cập**.
   - **Ngày thực thi**.
6. Nhấn **OK**.
7. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Bảo vệ email. Chống virus cho thư điện tử

Thành phần này có thể được sử dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Microsoft Windows cho máy trạm. Thành phần này không thể được sử dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Microsoft Windows cho máy chủ tập tin.

Mục này chứa thông tin về Chống virus cho thư điện tử và chỉ dẫn cách để thiết lập cấu hình thành phần.

Thông tin về Chống virus cho thư điện tử

Chống virus cho thư điện tử sẽ quét các email đến và đi để phát hiện virus và các mối đe dọa khác. Thành phần này được khởi động cùng với Kaspersky Endpoint Security, liên tục hoạt động trong bộ nhớ máy tính và quét tất cả các email được gửi hoặc nhận qua giao thức POP3, SMTP, IMAP, MAPI, và NNTP. Nếu không phát hiện mối đe dọa nào trong email, email đó sẽ có thể được truy cập và / hoặc xử lý.

Khi phát hiện một mối đe dọa trong một email, Chống virus cho thư điện tử sẽ thực hiện hành động sau:

1. Xác định loại đối tượng được phát hiện trong email (ví dụ như *trojan*).
2. Email sẽ được gán một trong các trạng thái sau:
   - *Có khả năng bị nhiễm*. Trạng thái này được gán nếu tác vụ quét không thể xác định liệu email đó có bị nhiễm hay không. Email có thể chứa một phần mã giống với một virus hoặc phần mềm độc hại khác, hoặc một bản sửa đổi của một virus đã biết.
   - *Bị nhiễm*. Trạng thái này được gán cho một đối tượng nếu tác vụ quét email phát hiện một phần mã của một virus đã biết được bao gồm trong cơ sở dữ liệu chống virus của Kaspersky Endpoint Security.
   - *Không tìm thấy*. Trạng thái này được gán cho một đối tượng nếu tác vụ quét email không phát hiện được virus hay các mối đe dọa khác.

Sau đó, ứng dụng sẽ chặn email, hiển thị một thông báo về đối tượng được phát hiện (nếu điều này được quy định trong cấu hình thông báo), và thực hiện hành động được quy định trong cấu hình Chống virus cho thư điện tử.

Thành phần này tương tác với trình khách email được cài đặt trên máy tính. Một phần mở rộng nhúng có thể được sử dụng cho trình khách email Microsoft Office Outlook®, cho phép bạn tinh chỉnh cấu hình quét email. Phần mở rộng Chống virus cho thư điện tử sẽ được nhúng trong trình khách Microsoft Office Outlook trong quá trình cài đặt Kaspersky Endpoint Security.

Hoạt động của Chống virus cho thư điện tử sẽ được thể hiện qua biểu tượng ứng dụng được hiển thị trong khu vực thông báo trên thanh tác vụ. Khi Chống virus cho thư điện tử đang quét một email, biểu tượng ứng dụng sẽ được đổi thành .

Bật và tắt Chống virus cho thư điện tử

Theo mặc định, Chống virus cho thư điện tử sẽ được bật và chạy trong một chế độ được khuyến nghị bởi các chuyên gia của Kaspersky. Bạn có thể tắt Chống virus cho thư điện tử nếu cần thiết.

Có hai cách để bật hoặc tắt thành phần này:

- Trên thẻ **Bảo vệ và Kiểm soát** của cửa sổ chính của ứng dụng
- Từ cửa sổ cấu hình ứng dụng.

Để bật hoặc tắt Chống virus cho thư điện tử trên thẻ Bảo vệ và Kiểm soát của cửa sổ chính của ứng dụng:

1. Mở cửa sổ chính của ứng dụng.
2. Chọn thẻ **Bảo vệ và Kiểm soát**.
3. Nhấn vào mục **Bảo vệ**.
   Mục **Bảo vệ** sẽ được mở ra.
4. Nhấn phải chuột để gọi menu ngữ cảnh của dòng có chứa thông tin về thành phần Chống virus cho thư điện tử.
   Một menu để chọn hành động đối với thành phần sẽ được mở ra.
5. Thực hiện một trong các thao tác sau:
   - Để bật Chống virus cho thư điện tử, chọn **Bắt đầu** trong menu.
     Biểu tượng trạng thái của thành phần , được hiển thị ở bên trái của dòng **Chống virus cho thư điện tử** sẽ được chuyển sang biểu tượng .
   - Để tắt Chống virus cho thư điện tử, chọn **Dừng** trong menu.
     Biểu tượng trạng thái của thành phần , được hiển thị ở bên trái của dòng **Chống virus cho thư điện tử** sẽ được chuyển sang biểu tượng .

Để bật hoặc tắt Chống virus cho thư điện tử từ cửa sổ cấu hình ứng dụng:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Chống virus cho thư điện tử**.
   Ở phần bên phải của cửa sổ, cấu hình của thành phần Chống virus cho thư điện tử sẽ được hiển thị.
3. Thực hiện một trong các thao tác sau:
   - Nếu bạn muốn bật Chống virus cho thư điện tử, chọn hộp kiểm **Bật Chống virus cho thư điện tử**.
   - Nếu bạn muốn tắt Chống virus cho thư điện tử, xóa hộp kiểm **Bật Chống virus cho thư điện tử**.
4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Thiết lập Chống virus cho thư điện tử

Bạn có thể làm như sau để thiết lập Chống virus cho thư điện tử:

- Thay đổi cấp độ bảo mật email.

Bạn có thể chọn một trong các cấp độ bảo mật email được thiết lập sẵn hoặc thiết lập một cấp độ bảo mật email tùy chỉnh.

Nếu bạn đã thay đổi cấu hình cấp độ bảo mật email, bạn luôn có thể hoàn tác lại đến cấu hình cấp độ bảo mật email được khuyến nghị.

- Thay đổi hành động được Kaspersky Endpoint Security thực hiện đối với các email bị nhiễm.
- Sửa phạm vi bảo vệ của Chống virus cho thư điện tử.
- Thiết lập quét các tập tin hỗn hợp được đính kèm email.

  Bạn có thể bật hoặc tắt tính năng quét các tập tin đính kèm email, giới hạn kích cỡ tối đa của các tập tin đính kèm email được quét, và giới hạn thời gian quét tối đa cho các tập tin đính kèm email.
- Thiết lập lọc theo kiểu tập tin đính kèm email.

  Lọc các tập tin đính kèm email theo kiểu cho phép tự động đổi tên hoặc xóa các tập tin thuộc những kiểu được quy định.
- Thiết lập Trình phân tích suy nghiệm.

  Để tăng hiệu quả bảo vệ, bạn có thể sử dụng phân tích suy nghiệm. Trong phân tích suy nghiệm, Kaspersky Endpoint Security sẽ phân tích hoạt động của các ứng dụng trong hệ điều hành. Phân tích suy nghiệm có thể phát hiện các mối đe dọa trong email chưa có hồ sơ trong cơ sở dữ liệu của Kaspersky Endpoint Security.
- Thiết lập quét email trong Microsoft Office Outlook.

  Một phần mở rộng nhúng có thể được sử dụng cho trình khách email Microsoft Office Outlook cho phép thiết lập dễ dàng cấu hình quét email.

  Khi làm việc với các trình khách email khác, bao gồm Microsoft Outlook Express®, Windows Mail, và Mozilla™ Thunderbird™, thành phần Chống virus cho thư điện tử sẽ quét lưu lượng của các giao thức SMTP, POP3, IMAP, và NNTP.

  > Khi làm việc với trình khách email Mozilla Thunderbird, Chống virus cho thư điện tử sẽ không quét các email được truyền qua giao thức IMAP để phát hiện virus và các mối đe dọa khác nếu bộ lọc được sử dụng để di chuyển email từ thư mục **Hộp thư đến**.

Thay đổi cấp độ bảo mật email

Chống virus cho thư điện tử sẽ áp dụng nhiều nhóm cấu hình khác nhau để bảo vệ email. Các nhóm cấu hình đó được gọi là *cấp độ bảo mật email*. Có 3 cấp độ bảo mật email: **Cao**, **Khuyên dùng**, và **Thấp**. Cấp độ bảo mật **Khuyên dùng** được coi là cấu hình tối ưu, và được khuyến nghị bởi Kaspersky.

Để thay đổi cấp độ bảo mật email:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Chống virus cho thư điện tử**.

   Ở phần bên phải của cửa sổ, cấu hình của thành phần Chống virus cho thư điện tử sẽ được hiển thị.
3. Trong mục **Mức độ bảo mật**, thực hiện một trong những hành động sau:

- Nếu bạn muốn cài đặt một trong những cấp độ bảo mật email được thiết lập sẵn (**Cao**, **Khuyên dùng**, hoặc **Thấp**), sử dụng thanh trượt để chọn.
- Nếu bạn muốn thiết lập một cấp độ bảo mật email tùy chỉnh, chọn nút **Cấu hình** và nhập cấu hình trong cửa sổ **Chống virus cho thư điện tử**.

  Sau khi bạn thiết lập một cấp độ bảo mật email tùy chỉnh, tên của cấp độ bảo mật trong mục **Mức độ bảo mật** sẽ được chuyển thành **Tùy chỉnh**.
- Nếu bạn muốn thay đổi cấp độ bảo mật email thành **Khuyên dùng**, nhấn nút **Mặc định**.

4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Thay đổi hành động xử lý các email bị nhiễm

Để thay đổi hành động xử lý các email bị nhiễm:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Chống virus cho thư điện tử**.

   Ở phần bên phải của cửa sổ, cấu hình của thành phần Chống virus cho thư điện tử sẽ được hiển thị.
3. Trong mục **Hành động khi phát hiện nguy hiểm**, chọn hành động mà Kaspersky Endpoint Security sẽ thực hiện khi phát hiện một email bị nhiễm:
   - **Lựa chọn hành động tự động**.
   - **Thực hiện hành động: Khử mã độc. Xóa nếu khử mã độc không thành công**.
   - **Thực hiện hành động: Khử mã độc**.
   - **Thực hiện hành động: Gỡ bỏ**.
   - **Thực hiện hành động: Ngăn chặn**.
4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Sửa phạm vi bảo vệ của Chống virus cho thư điện tử

Phạm vi bảo vệ nói đến các đối tượng được quét bởi thành phần khi thành phần này đang hoạt động. Phạm vi bảo vệ của các thành phần khác nhau có các thuộc tính khác nhau. Thuộc tính của phạm vi bảo vệ của Chống virus cho thư điện tử bao gồm cấu hình của Chống virus cho thư điện tử được tích hợp vào các trình khách email, và loại email và giao thức email có lưu lượng được quét bởi Chống virus cho thư điện tử. Theo mặc định, Kaspersky Endpoint Security sẽ quét cả hai loại email đến và đi, cũng như lưu lượng của các giao thức POP3, SMTP, NNTP và IMAP, và được tích hợp vào trình khách email Microsoft Office Outlook.

Để tạo phạm vi bảo vệ của Chống virus cho thư điện tử:

1. Mở cửa sổ cấu hình ứng dụng.

2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Chống virus cho thư điện tử**.

   Ở phần bên phải của cửa sổ, cấu hình của thành phần Chống virus cho thư điện tử sẽ được hiển thị.

3. Nhấn nút **Cấu hình**.

   Cửa sổ **Chống virus cho thư điện tử** sẽ được mở ra.

4. Chọn thẻ **Tổng quát**.

5. Trong mục **Phạm vi bảo vệ**, thực hiện một trong các thao tác sau:

   - Nếu bạn muốn Chống virus cho thư điện tử quét tất cả các email đến và đi trên máy tính của mình, chọn **Tin nhắn gửi đến và gửi đi**.

   - Nếu bạn muốn Chống virus cho thư điện tử chỉ quét các email đến trên máy tính của mình, chọn **Chỉ tin nhắn gửi đến**.

     Nếu bạn chọn chỉ quét những email đến, bạn nên thực hiện tác vụ quét một lần cho tất cả những email đi bởi sẽ có khả năng máy tính của bạn có sâu email đang được phát tán qua email. Điều này để tránh các vấn đề xuất phát từ việc gửi hàng loạt email không giám sát bị nhiễm virus từ máy tính của bạn.

6. Trong mục **Khả năng kết nối**, thực hiện các thao tác sau:

   - Nếu bạn muốn Chống virus cho thư điện tử quét các email được truyền qua các giao thức POP3, SMTP, NNTP và IMAP trước khi chúng đến máy tính của bạn, chọn hộp kiểm **lưu lượng POP3 / SMTP / NNTP / IMAP**.

     Nếu bạn không muốn Chống virus cho thư điện tử quét các email được truyền qua các giao thức POP3, SMTP, NNTP và IMAP trước khi chúng đến máy tính của bạn, xóa hộp kiểm **Lưu lượng POP3 / SMTP / NNTP / IMAP**. Trong trường hợp này, các email sẽ được quét bởi phần mở rộng Chống virus cho thư điện tử được nhúng trong trình khách email Microsoft Office Outlook sau khi email đó đã đến máy tính của người dùng nếu hộp kiểm **Bổ sung: Phần mở rộng Microsoft Office Outlook** được chọn.

     Nếu bạn sử dụng một trình khách email ngoài Microsoft Office Outlook, các email được truyền qua các giao thức POP3, SMTP, NNTP và IMAP sẽ không được quét bởi Chống virus cho thư điện tử khi hộp kiểm **Lưu lượng POP3 / SMTP / NNTP / IMAP** bị xóa.

   - Nếu bạn muốn cho phép truy cập đến cấu hình Chống virus cho thư điện tử từ Microsoft Office Outlook và bật tính năng quét các email được truyền qua các giao thức POP3, SMTP, NNTP, IMAP, và MAPI sau khi chúng đã đến máy tính sử dụng phần mở rộng được nhúng vào Microsoft Office Outlook, hãy chọn hộp kiểm **Bổ sung: Phần mở rộng Microsoft Office Outlook**.

     Nếu bạn muốn chặn truy cập đến cấu hình Chống virus cho thư điện tử từ Microsoft Office Outlook và tắt tính năng quét các email được truyền qua các giao thức POP3, SMTP, NNTP, IMAP, và MAPI sau khi chúng đã đến máy tính sử dụng phần mở rộng được nhúng vào Microsoft Office Outlook, hãy xóa hộp kiểm **Bổ sung: Phần mở rộng Microsoft Office Outlook**.

     Phần mở rộng Chống virus cho thư điện tử sẽ được nhúng trong trình khách Microsoft Office Outlook trong quá trình cài đặt Kaspersky Endpoint Security.

7. Nhấn **OK**.

8. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Quét các tập tin hỗn hợp được đính kèm email

Để thiết lập quét các tập tin hỗn hợp được đính kèm email:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Chống virus cho thư điện tử**.

   Ở phần bên phải của cửa sổ, cấu hình của thành phần Chống virus cho thư điện tử sẽ được hiển thị.
3. Nhấn nút **Cấu hình**.

   Cửa sổ **Chống virus cho thư điện tử** sẽ được mở ra.
4. Chọn thẻ **Tổng quát**.
5. Thực hiện hành động sau trong mục **Quét các tập tin hỗn hợp**:

   - Nếu bạn muốn Chống virus cho thư điện tử bỏ qua các tập nén được đính kèm email, hãy xóa hộp kiểm **Quét tập tin đính kèm**.
   - Nếu bạn muốn Chống virus cho thư điện tử bỏ qua các tập tin đính kèm email lớn hơn N megabyte, hãy chọn hộp kiểm **Không quét tập nén lớn hơn N MB**. Nếu bạn chọn hộp kiểm này, hãy quy định kích cỡ tập nén tối đa trong trường đối diện tên của hộp kiểm.
   - Nếu bạn muốn Chống virus cho thư điện tử quét các tập tin đính kèm email cần nhiều hơn N giây để quét, hãy xóa hộp kiểm **Không quét tập tin nhiều hơn N giây**.
6. Nhấn **OK**.
7. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Lọc các tập tin đính kèm email

Các chương trình độc hại có thể được phân phối dưới dạng tập tin đính kèm trong email. Bạn có thể thiết lập bộ lọc dựa trên loại tập tin đính kèm email, để các tập tin thuộc kiểu được quy định được tự động đổi tên hoặc xóa. Bằng cách đổi tên một tập tin đính kèm thuộc một thể loại nhất định, Kaspersky Endpoint Security có thể bảo vệ máy tính của bạn chống lại việc tự động thực thi một chương trình độc hại.

Để thiết lập bộ lọc tập tin đính kèm:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Chống virus cho thư điện tử**.

   Ở phần bên phải của cửa sổ, cấu hình của thành phần Chống virus cho thư điện tử sẽ được hiển thị.
3. Trong mục **Mức độ bảo mật**, nhấn nút **Cấu hình**.

Cửa sổ **Chống virus cho thư điện tử** sẽ được mở ra.

4. Trong cửa sổ **Chống virus cho thư điện tử**, chọn thẻ **Lọc tập tin đính kèm**.

5. Thực hiện một trong các thao tác sau:

   - Nếu bạn không muốn Chống virus cho thư điện tử lọc các tập tin đính kèm email, chọn **Vô hiệu lọc**.

   - Nếu bạn muốn Chống virus cho thư điện tử đổi tên các tập tin đính kèm email thuộc **kiểu được quy định**, chọn **Đổi tên loại tập tin đính kèm được chỉ định**.

Lưu ý rằng định dạng thực tế của một tập tin có thể không khớp với phần mở rộng của tên tập tin đó.

Nếu bạn bật tính năng lọc các đối tượng được đính kèm email, Chống virus cho thư điện tử có thể đổi tên hoặc xóa các tập tin có các phần mở rộng sau:

com – tập tin thực thi của một ứng dụng nhỏ hơn hoặc bằng 64 KB

exe – tập tin thực thi hoặc tập nén tự trích xuất

sys – tập tin hệ thống Microsoft Windows

prg – văn bản chương trình cho dBase™, Clipper hoặc Microsoft Visual FoxPro®, hay một chương trình WAVmaker

bin – tập tin nhị phân

bat – tập tin xử lý theo lô

cmd – tập tin lệnh cho Microsoft Windows NT (tương đương tập tin bat cho DOS), OS/2

dpl – thư viện nén của Borland Delphi

dll – thư viện liên kết động

scr – màn hình khởi động của Microsoft Windows

cpl – mô-đun control panel của Microsoft Windows

ocx – đối tượng Microsoft OLE (Liên kết và Nhúng Đối tượng)

tsp – chương trình đang chạy trong chế độ chia thời gian

drv – trình điều khiển thiết bị

vxd – trình điều khiển thiết bị ảo Microsoft Windows

pif – tập tin thông tin chương trình

lnk – tập tin liên kết Microsoft Windows

reg – tập tin khóa registry hệ thống Microsoft Windows

ini – tập tin thiết lập có chứa dữ liệu thiết lập cho Microsoft Windows, Windows NT, và một số ứng dụng khác

cla – lớp Java

vbs – kịch bản Visual Basic®

vbe – phần mở rộng video BIOS

js, jse – mã nguồn JavaScript

htm – tài liệu siêu văn bản

htt – đầu đề siêu văn bản Microsoft Windows

hta – chương trình siêu văn bản cho Microsoft Internet Explorer®

asp – kịch bản Active Server Pages

chm – tập tin HTML đã biên dịch

pht – tập tin HTML có tích hợp kịch bản PHP

php – kịch bản được tích hợp vào tập tin HTML

wsh – tập tin Microsoft Windows Script Host

wsf – kịch bản Microsoft Windows

the – tập tin hình nền màn hình làm việc cho Microsoft Windows 95

hlp – tập tin Trợ giúp Win

eml – thư Microsoft Outlook Express

nws – email mới của Microsoft Outlook Express

msg – email Microsoft Mail

plg – email

mbx – phần mở rộng cho một email Microsoft Office Outlook được lưu

doc* – tài liệu Microsoft Office Word, ví dụ: doc cho tài liệu Microsoft Office Word, docx cho tài liệu Microsoft Office Word 2007 với hỗ trợ XML, và docm cho tài liệu Microsoft Office Word 2007 với hỗ trợ macro

dot* – mẫu tài liệu Microsoft Office Word, ví dụ như: dot cho mẫu tài liệu Microsoft Office Word, dotx cho mẫu tài liệu Microsoft Office Word 2007, dotm cho mẫu tài liệu Microsoft Office Word 2007 với hỗ trợ macro

fpm – tập tin bắt đầu cho chương trình cơ sở dữ liệu, Microsoft Visual FoxPro

rtf – tài liệu Văn bản Giàu Tính chất

shs – phân mảnh Windows Shell Scrap Object Handler

dwg – cơ sở dữ liệu vẽ AutoCAD®

msi – gói Microsoft Windows Installer

otm – dự án VBA cho Microsoft Office Outlook

pdf – tài liệu Adobe Acrobat

swf – đối tượng đóng gói Shockwave® Flash

jpg, jpeg – định dạng đồ họa hình ảnh được nén

emf – tập tin định dạng Enhanced Metafile. Thế hệ kế tiếp của siêu tập tin hệ điều hành Microsoft Windows. Các tập tin EMF không được hỗ trợ bởi Microsoft Windows 16 bit.

ico – tập tin biểu tượng đối tượng

ov? – tập tin thực thi của Microsoft Office Word

xl* – tài liệu và tập tin Microsoft Office Excel, ví dụ như: xla, phần mở rộng cho Microsoft Office Excel, xlc cho biểu đồ, xlt cho mẫu tài liệu, xlsx cho sổ làm việc Microsoft Office Excel 2007, xltm cho sổ làm việc Microsoft Office Excel 2007 với hỗ trợ macro, xlsb cho sổ làm việc Microsoft Office Excel 2007 trong định dạng nhị phân (phi XML), xltx cho mẫu Microsoft Office Excel 2007, xlsm cho mẫu Microsoft Office Excel 2007 với hỗ trợ macro, và xlam cho tiện ích Microsoft Office Excel 2007 với hỗ trợ macro

pp* – tài liệu và tập tin Microsoft Office PowerPoint®, ví dụ như: pps cho các trang Microsoft Office PowerPoint slides, ppt cho thuyết trình, pptx cho thuyết trình Microsoft Office PowerPoint 2007, pptm cho thuyết trình Microsoft Office PowerPoint 2007 với hỗ trợ macro, potx cho mẫu thuyết trình Microsoft Office PowerPoint 2007, potm cho mẫu thuyết trình Microsoft Office PowerPoint 2007 với hỗ trợ macro, ppsx cho slideshow Microsoft Office PowerPoint 2007, ppsm cho slideshow Microsoft Office PowerPoint 2007 với hỗ trợ macro, và ppam cho tiện ích Microsoft Office PowerPoint 2007 với hỗ trợ macro

md* – tài liệu và tập tin Microsoft Office Access®, ví dụ như: mda cho nhóm làm việc Microsoft Office Access và mdb cho cơ sở dữ liệu

sldx – một trang Microsoft PowerPoint 2007

sldm – một trang Microsoft PowerPoint 2007 với hỗ trợ macro

thmx – một chủ đề Microsoft Office 2007

- Nếu bạn muốn Chống virus cho thư điện tử xóa các tập tin đính kèm email thuộc kiểu được quy định, chọn **Xóa loại tập tin đính kèm được chỉ định**.

6. Nếu bạn đã chọn **Đổi tên loại tập tin đính kèm được chỉ định** hoặc **Xóa loại tập tin đính kèm được chỉ định** ở bước trước, hãy chọn hộp kiểm đối diện các loại tập tin tương ứng.

   Bạn có thể thay đổi danh sách các loại tập tin bằng cách sử dụng các nút **Thêm**, **Sửa** và **Gỡ bỏ**.

7. Nhấn **OK**.

8. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Quét email trong Microsoft Office Outlook

Trong quá trình cài đặt Kaspersky Endpoint Security, phần mở rộng Chống virus cho thư điện tử sẽ được nhúng vào Microsoft Office Outlook (sau đây còn được gọi là Outlook). Nó cho phép bạn mở cấu hình Chống virus cho thư điện tử từ trong Outlook, và quy định khi nào thì email được quét để phát hiện virus và các mối đe dọa khác. Phần mở rộng Chống virus cho thư điện tử cho Outlook có thể quét các email đến và đi được truyền tải qua các giao thức POP3, SMTP, NNTP, IMAP, và MAPI.

Cấu hình Chống virus cho thư điện tử có thể được thiết lập trực tiếp trong Outlook nếu hộp kiểm **Bổ sung: Phần mở rộng Microsoft Office Outlook** được chọn trong giao diện của Kaspersky Endpoint Security.

Trong Outlook, các email vào sẽ được quét đầu tiên bởi Chống virus cho thư điện tử (nếu hộp kiểm **lưu lượng POP3 / SMTP / NNTP / IMAP** được chọn trong giao diện của Kaspersky Endpoint Security) và sau đó là bởi phần mở rộng Chống virus cho thư điện tử cho Outlook. Nếu Chống virus cho thư điện tử phát hiện một đối tượng độc hại trong email, thành phần này sẽ cảnh báo cho bạn về sự kiện này.

Hành động được lựa chọn của bạn trong cửa sổ thông báo sẽ xác định thành phần nào được sử dụng để loại trừ mối đe dọa trong email: Chống virus cho thư điện tử hoặc phần mở rộng Chống virus cho thư điện tử cho Outlook.

- Nếu bạn chọn **Khử mã độc** hoặc **Gỡ bỏ** trong cửa sổ thông báo, việc loại trừ mối đe dọa sẽ được thực hiện bởi Chống virus cho thư điện tử.
- Nếu bạn chọn **Bỏ qua** trong cửa sổ thông báo người dùng, phần mở rộng Chống virus cho thư điện tử cho Outlook sẽ loại trừ mối đe dọa.

Các email ra được quét đầu tiên bởi phần mở rộng Chống virus cho thư điện tử cho Outlook, và sau đó được quét bởi Chống virus cho thư điện tử.

Thiết lập quét email trong Outlook

Để thiết lập quét email trong Outlook 2007:

1. Mở cửa sổ chính của Outlook 2007.
2. Chọn **Service** (Dịch vụ) → **Settings** (Cấu hình) từ thanh menu.
   Cửa sổ **Options** (Tùy chọn) sẽ được mở ra.
3. Trong cửa sổ **Options** (Tùy chọn), chọn thẻ **Email protection** (Bảo vệ email).

Để thiết lập quét email trong Outlook 2010 / 2013:

1. Mở cửa sổ chính của Outlook.
   Chọn thẻ **File** (Tập tin) ở góc trên bên trái.
2. Nhấn nút **Options** (Tùy chọn).
   Cửa sổ **Outlook Options** (Tùy chọn của Outlook) sẽ được mở ra.
3. Chọn mục **Add-Ins** (Tiện ích).
   Cấu hình của các tiện ích được nhúng vào Outlook sẽ được hiển thị ở phần bên phải của cửa sổ.
4. Nhấn nút **Add-In Options** (Tùy chọn Tiện ích).

Thiết lập quét email sử dụng Kaspersky Security Center

Nếu email được quét sử dụng phần mở rộng Chống virus cho thư điện tử cho Outlook, bạn nên sử dụng Cached Exchange Mode (Chế độ bộ nhớ đệm cho Exchange). Để biết thêm chi tiết về Cached Exchange Mode và các khuyến nghị sử dụng của nó, hãy tham khảo Cơ sở Tri thức của Microsoft: https://technet.microsoft.com/en-us/library/cc179175.aspx.

Để thiết lập chế độ hoạt động của phần mở rộng Chống virus cho thư điện tử cho Outlook sử dụng Kaspersky Security Center:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, mở thư mục với tên của nhóm quản trị mà bạn muốn thiết lập tác vụ quét email.
3. Trong không gian làm việc, chọn thẻ **Chính sách**.
4. Chọn chính sách cần thiết.
5. Mở cửa sổ **Thuộc tính: <Tên chính sách>** sử dụng một trong những phương pháp sau đây:
   - Trong menu ngữ cảnh của chính sách, chọn **Thuộc tính**.
   - Nhấn vào liên kết **Thiết lập chính sách** được đặt ở phần bên phải của không gian làm việc của Bảng điều khiển Quản trị.
6. Trong mục **Bảo vệ Chống virus**, chọn mục con **Chống virus cho thư điện tử**.
7. Trong mục **Mức độ bảo mật**, nhấn nút **Cấu hình**.
   Cửa sổ **Chống virus cho thư điện tử** sẽ được mở ra.
8. Trong mục **Khả năng kết nối**, nhấn nút **Cấu hình**.
   Cửa sổ **Bảo vệ email** sẽ được mở ra.
9. Trong cửa sổ **Bảo vệ email**:
   - Chọn hộp kiểm **Quét khi nhận** nếu bạn muốn phần mở rộng Chống virus cho thư điện tử cho Outlook quét các email đến khi chúng vào hộp thư.
   - Chọn hộp kiểm **Quét khi đọc** nếu bạn muốn phần mở rộng Chống virus cho thư điện tử cho Outlook quét các email đến khi người sử dụng đọc chúng.
   - Chọn hộp kiểm **Quét khi gửi** nếu bạn muốn phần mở rộng Chống virus cho thư điện tử cho Outlook quét các email đi khi chúng được gửi.
10. Trong cửa sổ **Bảo vệ email**, nhấn **OK**.
11. Trong cửa sổ **Chống virus cho thư điện tử**, nhấn **OK**.
12. Áp dụng chính sách.

Xem *Hướng dẫn dành cho Quản trị viên Kaspersky Security Center* để biết chi tiết về việc áp dụng các chính sách Kaspersky Security Center.

Bảo vệ máy tính trên Internet. Chống virus cho web

Thành phần này có thể được sử dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Microsoft Windows cho máy trạm. Thành phần này không thể được sử dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Microsoft Windows cho máy chủ tập tin.

Mục này chứa thông tin về Chống virus cho web và chỉ dẫn cách để thiết lập cấu hình thành phần.

Thông tin về Chống virus cho web

Mỗi khi bạn lên mạng, bạn sẽ có nguy cơ tiết lộ thông tin được lưu trữ trên máy tính của mình đến cho virus và các phần mềm độc hại khác. Chúng có thể xâm nhập máy tính trong khi người dùng tải về các phần mềm miễn phí, hoặc duyệt các website bị khống chế bởi tội phạm. Các loại sâu mạng có thể tìm đường vào máy tính của bạn ngay khi bạn thiết lập một kết nối Internet, kể cả trước khi bạn mở ra trang web hoặc tải về một tập tin.

Chống virus cho web bảo vệ dữ liệu vào và ra được gửi đến và từ máy tính của bạn qua các giao thức HTTP và FTP, đồng thời đối chiếu các URL với danh sách những địa chỉ web độc hại hoặc lừa đảo.

Chống virus cho web sẽ theo dõi và phân tích để phát hiện virus và các mối đe dọa khác trên mọi trang web và tập tin được truy cập bởi người dùng hoặc một ứng dụng thông qua giao thức HTTP và FTP. Những điều sau đây có thể xảy ra:

- Nếu một trang hoặc tập tin được phát hiện là không chứa mã độc, người dùng sẽ có thể truy cập chúng ngay lập tức.
- Nếu người dùng truy cập một trang web hoặc tập tin có chứa mã độc, ứng dụng sẽ thực hiện hành động được quy định trong cấu hình Chống virus cho web.

Bật và tắt Chống virus cho web

Theo mặc định, Chống virus cho web sẽ được bật và chạy trong một chế độ được khuyến nghị bởi các chuyên gia của Kaspersky. Bạn có thể tắt Chống virus cho web nếu cần thiết.

Có hai cách để bật hoặc tắt thành phần này:

- Trên thẻ **Bảo vệ và Kiểm soát** của cửa sổ chính của ứng dụng
- Từ cửa sổ cấu hình ứng dụng.

Để bật hoặc tắt Chống virus cho web trên thẻ Bảo vệ và Kiểm soát của cửa sổ chính của ứng dụng:

1. Mở cửa sổ chính của ứng dụng.
2. Chọn thẻ **Bảo vệ và Kiểm soát**.
3. Nhấn vào mục **Bảo vệ**.
   Mục **Bảo vệ** sẽ được mở ra.

4. Nhấn phải chuột để gọi menu ngữ cảnh của dòng có chứa thông tin về thành phần Chống virus cho web.

   Một menu để chọn hành động đối với thành phần sẽ được mở ra.

5. Thực hiện một trong các thao tác sau:

   - Để bật Chống virus cho web, chọn **Bắt đầu** trong menu.

     Biểu tượng trạng thái của thành phần , được hiển thị ở bên trái của dòng **Chống virus cho web** sẽ được chuyển sang biểu tượng .

   - Để tắt Chống virus cho web, chọn **Dừng** trong menu.

     Biểu tượng trạng thái của thành phần , được hiển thị ở bên trái của dòng **Chống virus cho web** sẽ được chuyển sang biểu tượng .

Để bật hoặc tắt Chống virus cho web từ cửa sổ cấu hình ứng dụng:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Chống virus cho web**.

   Ở phần bên phải của cửa sổ, cấu hình của thành phần Chống virus cho web sẽ được hiển thị.

3. Thực hiện một trong các thao tác sau:

   - Nếu bạn muốn bật Chống virus cho web, chọn hộp kiểm **Bật Chống virus cho web**.
   - Nếu bạn muốn tắt Chống virus cho web, xóa hộp kiểm **Bật Chống virus cho web**.

4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Thiết lập Chống virus cho web

Bạn có thể làm như sau để thiết lập cho Chống virus cho web:

- Thay đổi cấp độ bảo mật lưu lượng web.

  Bạn có thể chọn một trong nhiều cấp độ bảo mật được cài đặt sẵn cho lưu lượng web được nhận hoặc truyền tải qua các giao thức HTTP và FTP, hoặc thiết lập một cấp độ bảo mật tùy chỉnh cho lưu lượng web.

  Nếu bạn đã thay đổi cấu hình cấp độ bảo mật lưu lượng web, bạn luôn có thể hoàn tác lại đến cấu hình cấp độ bảo mật lưu lượng web được khuyến nghị.

- Thay đổi hành động được Kaspersky Endpoint Security thực hiện khi phát hiện các đối tượng web độc hại.

  Nếu việc phân tích một đối tượng HTTP cho thấy nó có chứa mã độc, phản ứng của Chống virus cho web sẽ tùy thuộc vào hành động mà bạn đã quy định.

- Thiết lập tính năng đối chiếu các URL với cơ sở dữ liệu các địa chỉ web lừa đảo và độc hại của Chống virus cho web.

- Thiết lập việc sử dụng phân tích suy nghiệm khi quét lưu lượng web để tìm virus và các chương trình độc hại khác.

Để tăng hiệu quả bảo vệ, bạn có thể sử dụng phân tích suy nghiệm. Trong phân tích suy nghiệm, Kaspersky Endpoint Security sẽ phân tích hoạt động của các ứng dụng trong hệ điều hành. Phân tích suy nghiệm có thể phát hiện các mối đe dọa chưa có hồ sơ trong cơ sở dữ liệu của Kaspersky Endpoint Security.

- Thiết lập việc sử dụng phân tích suy nghiệm khi quét lưu lượng web để tìm các liên kết lừa đảo.
- Tối ưu tính năng quét lưu lượng web được đến và đi thông qua các giao thức HTTP và FTP của Chống virus cho web.
- Tạo một danh sách các URL được tin tưởng.

  Bạn có thể tạo ra một danh sách các URL có nội dung mà bạn tin tưởng. Chống virus cho web sẽ không phân tích thông tin từ các URL được tin tưởng để phát hiện virus và các mối đe dọa khác. Tùy chọn này có thể hữu ích, chẳng hạn như khi Chống virus cho web can thiệp với việc tải về một tập tin từ một website đã biết.

  Một URL có thể là địa chỉ của một trang web cụ thể, hoặc địa chỉ của một website.

Thay đổi cấp độ bảo mật lưu lượng web

Để bảo vệ dữ liệu được nhận và truyền tải thông qua các giao thức HTTP và FTP, Chống virus cho web sẽ áp dụng nhiều nhóm cấu hình khác nhau. Các nhóm cấu hình này được gọi là *cấp độ bảo mật lưu lượng web*. Có 3 cấp độ bảo mật lưu lượng web được thiết lập sẵn: **Cao**, **Khuyên dùng**, và **Thấp**. Cấp độ bảo mật lưu lượng web **Khuyên dùng** được coi là cấu hình tối ưu, và được khuyến nghị bởi Kaspersky.

Để thay đổi cấp độ bảo mật lưu lượng web:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Chống virus cho web**.

   Ở phần bên phải của cửa sổ, cấu hình của thành phần Chống virus cho web sẽ được hiển thị.
3. Trong mục **Mức độ bảo mật**, thực hiện một trong những hành động sau:
   - Nếu bạn muốn cài đặt một trong những cấp độ bảo mật lưu lượng web được thiết lập sẵn (**Cao**, **Khuyên dùng**, hoặc **Thấp**), sử dụng thanh trượt để chọn.
   - Nếu bạn muốn thiết lập một cấp độ bảo mật lưu lượng web tùy chỉnh, chọn nút **Cấu hình** và nhập cấu hình trong cửa sổ **Chống virus cho web**.

     Khi bạn đã thiết lập một cấp độ bảo mật lưu lượng web tùy chỉnh, tên của cấp độ bảo mật trong mục **Mức độ bảo mật** sẽ được chuyển thành **Tùy chỉnh**.
   - Nếu bạn muốn thay đổi cấp độ bảo mật lưu lượng web thành **Khuyên dùng**, nhấn nút **Mặc định**.
4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Thay đổi hành động xử lý các đối tượng lưu lượng web độc hại

Để thay đổi hành động xử lý các đối tượng lưu lượng web độc hại:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Chống virus cho web**.
   Ở phần bên phải của cửa sổ, cấu hình của thành phần Chống virus cho web sẽ được hiển thị.
3. Trong mục **Hành động khi phát hiện nguy hiểm**, chọn hành động được Kaspersky Endpoint Security thực hiện khi phát hiện các đối tượng web độc hại:
   - **Lựa chọn hành động tự động**.
   - **Ngăn chặn tải về**.
   - **Cho phép tải về**.
4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Chống virus cho web sẽ đối chiếu các URL với cơ sở dữ liệu các địa chỉ web lừa đảo và độc hại.

Việc quét liên kết để xem chúng có được bao gồm trong danh sách các địa chỉ web lừa đảo hay không cho phép bạn tránh *các cuộc tấn công lừa đảo*. Một cuộc tấn công lừa đảo có thể bị che giấu, chẳng hạn như dưới dạng một email từ ngân hàng của bạn, với liên kết đến website chính thức của ngân hàng. Bằng cách nhấn vào liên kết đó, bạn sẽ được đưa đến một bản sao chính xác của website ngân hàng và thậm chí còn có thể thấy đúng địa chỉ web của ngân hàng đó trong trình duyệt, mặc dù trong thực tế bạn đang ở trên một website giả mạo. Kể từ thời điểm này, mọi hành động của bạn trên website đều sẽ được theo dõi và có thể được sử dụng để ăn cắp tiền của bạn.

Bởi các liên kết đến website lừa đảo có thể được nhận không chỉ qua email, mà còn từ các nguồn khác như tin nhắn ICQ, Chống virus cho web sẽ giám sát mọi nỗ lực truy cập một website lừa đảo trên cấp độ lưu lượng web và chặn việc truy cập đến các website đó. Danh sách các URL được bao gồm với gói phân phối của Kaspersky Endpoint Security.

Để thiết lập tính năng đối chiếu các URL với cơ sở dữ liệu các địa chỉ web lừa đảo và độc hại của Chống virus cho web:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Chống virus cho web**.
   Ở phần bên phải của cửa sổ, cấu hình của thành phần Chống virus cho web sẽ được hiển thị.
3. Nhấn nút **Cấu hình**.
   Cửa sổ **Chống virus cho web** sẽ được mở ra.
4. Trong cửa sổ **Chống virus cho web**, chọn thẻ **Tổng quát**.
5. Làm các bước sau:
   - Nếu bạn muốn Chống virus cho web đối chiếu các URL với cơ sở dữ liệu các địa chỉ web độc hại, trong mục **Phương thức quét**, chọn hộp kiểm **Kiểm tra nếu liên kết được liệt kê trong cơ sở dữ liệu liên kết độc hại**.

- Nếu bạn muốn Chống virus cho web đối chiếu các URL với cơ sở dữ liệu các địa chỉ web lừa đảo, trong mục **Cấu hình chống lừa đảo**, chọn hộp kiểm **Kiểm tra nếu liên kết được liệt kê trong cơ sở dữ liệu liên kết độc hại**.

Bạn cũng có thể đối chiếu các liên kết với cơ sở dữ liệu danh tiếng của Kaspersky Security Network.

6. Nhấn **OK**.
7. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Sử dụng Trình phân tích suy nghiệm với Chống virus cho web

Để thiết lập sử dụng phân tích suy nghiệm:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Chống virus cho web**.
   Ở phần bên phải của cửa sổ, cấu hình của thành phần Chống virus cho web sẽ được hiển thị.
3. Trong mục **Mức độ bảo mật**, nhấn nút **Cấu hình**.
   Cửa sổ **Chống virus cho web** sẽ được mở ra.
4. Chọn thẻ **Tổng quát**.
5. Nếu bạn muốn Chống virus cho web sử dụng phân tích suy nghiệm để quét lưu lượng web để phát hiện virus và các phần mềm độc hại khác, trong mục **Phương thức quét**, chọn hộp kiểm **Phân tích theo hành vi để phát hiện virus** và sử dụng thanh trượt để đặt cấp độ phân tích suy nghiệm: **Quét nhanh**, **quét vừa**, hoặc **quét kỹ**.
6. Nếu bạn muốn Chống virus cho web sử dụng phân tích suy nghiệm để quét các trang web và phát hiện liên kết lừa đảo, trong mục **Cấu hình chống lừa đảo**, chọn hộp kiểm **Phân tích theo hành vi để phát hiện liên kết lừa đảo**
7. Nhấn **OK**.
8. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Sửa danh sách các URL tin tưởng

Để tạo một danh sách các URL được tin tưởng:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Chống virus cho web**.
   Ở phần bên phải của cửa sổ, cấu hình của thành phần Chống virus cho web sẽ được hiển thị.
3. Nhấn nút **Cấu hình**.

Cửa sổ **Chống virus cho web** sẽ được mở ra.

4. Chọn thẻ **URL được tin tưởng**.
5. Chọn hộp kiểm **Không quét lưu lượng web từ các địa chỉ web được tin tưởng**.
6. Tạo một danh sách các URL / trang web có nội dung mà bạn tin tưởng. Để tạo một danh sách:
   a. Nhấn vào nút **Thêm**.
      Cửa sổ **Địa chỉ web / Địa chỉ đại diện web** sẽ được mở ra.
   b. Nhập địa chỉ của website / trang web hoặc mặt nạ địa chỉ của website / trang web.
   c. Nhấn **OK**.
      Một hồ sơ mới sẽ xuất hiện trong danh sách các URL được tin tưởng.
7. Nhấn **OK**.
8. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Bảo vệ lưu lượng của ứng dụng nhắn tin nhanh. Chống virus cho tin nhắn

Thành phần này có thể được sử dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Microsoft Windows cho máy trạm. Thành phần này không thể được sử dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Microsoft Windows cho máy chủ tập tin.

Phần này chứa thông tin về Chống virus cho tin nhắn và chỉ dẫn cách để thiết lập cấu hình thành phần.

Thông tin về Chống virus cho tin nhắn

Chống virus cho tin nhắn sẽ quét lưu lượng của các trình khách nhắn tin nhanh (còn được gọi là *các ứng dụng nhắn tin nhanh*).

Chống virus cho tin nhắn sẽ không quét các tin nhắn được truyền qua những kênh được mã hóa.

Các tin nhắn được gửi qua ứng dụng nhắn tin nhanh có thể chứa các mối đe dọa bảo mật sau đây:

- Các URL tìm cách tải về một chương trình độc hại lên máy tính
- Các URL đến những chương trình độc hại và website mà kẻ xâm nhập sử dụng để tấn công lừa đảo

  Mục tiêu của các cuộc tấn công lừa đảo là đánh cắp dữ liệu cá nhân của người dùng, ví dụ như số thẻ ngân hàng, thông tin hộ chiếu, mật khẩu cho các hệ thống thanh toán ngân hàng và các dịch vụ trực tuyến khác (ví dụ như các website mạng xã hội hoặc tài khoản email).

Các tập tin có thể được truyền tải thông qua ứng dụng nhắn tin nhanh. Khi người dùng cố gắng lưu lại các tập tin đó, các tập tin sẽ được quét bởi thành phần Chống virus cho tập tin.

Chống virus cho tin nhắn sẽ theo dõi mọi tin nhắn được người dùng gửi hoặc nhận thông qua ứng dụng nhắn tin nhanh và quét nó để phát hiện các liên kết có thể đe dọa sự bảo mật của máy tính:

- Nếu không có URL nguy hiểm nào được phát hiện trong tin nhắn, nó sẽ được chuyển đến người dùng.
- Nếu có các liên kết nguy hiểm trong tin nhắn, Chống virus cho tin nhắn sẽ thay thế tin nhắn này với thông tin về mối đe dọa trong cửa sổ nhắn tin của ứng dụng nhắn tin nhanh đang hoạt động.

Bật và tắt Chống virus cho tin nhắn

Theo mặc định, Chống virus cho tin nhắn sẽ được bật và chạy trong một chế độ được khuyến nghị bởi các chuyên gia của Kaspersky. Bạn có thể tắt Chống virus cho tin nhắn nếu cần thiết.

Có hai cách để bật hoặc tắt thành phần này:

- Trên thẻ **Bảo vệ và Kiểm soát** của cửa sổ chính của ứng dụng

- Từ cửa sổ cấu hình ứng dụng.

Để bật hoặc tắt Chống virus cho tin nhắn trên thẻ Bảo vệ và Kiểm soát của cửa sổ chính của ứng dụng:

1. Mở cửa sổ chính của ứng dụng.
2. Chọn thẻ **Bảo vệ và Kiểm soát**.
3. Nhấn vào mục **Bảo vệ**.

   Mục **Bảo vệ** sẽ được mở ra.
4. Nhấn phải chuột lên dòng **Chống virus cho tin nhắn** để hiển thị menu ngữ cảnh của hành động của thành phần.
5. Thực hiện một trong các thao tác sau:

   - Để bật Chống virus cho tin nhắn, chọn **Bắt đầu** trong menu ngữ cảnh.

     Biểu tượng trạng thái của thành phần , được hiển thị ở bên trái của dòng **Chống virus cho tin nhắn** sẽ được chuyển sang biểu tượng .
   - Để tắt Chống virus cho tin nhắn, chọn **Dừng** trong menu ngữ cảnh.

     Biểu tượng trạng thái của thành phần , được hiển thị ở bên trái của dòng **Chống virus cho tin nhắn** sẽ được chuyển sang biểu tượng .

Để bật hoặc tắt Chống virus cho tin nhắn từ cửa sổ cấu hình ứng dụng:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Chống virus cho tin nhắn**.

   Ở phần bên phải của cửa sổ, cấu hình của thành phần Chống virus cho tin nhắn sẽ được hiển thị.
3. Thực hiện một trong các thao tác sau:

   - Nếu bạn muốn bật Chống virus cho tin nhắn, chọn hộp kiểm **Bật Chống virus cho tin nhắn**.
   - Nếu bạn muốn tắt Chống virus cho tin nhắn, xóa hộp kiểm **Bật Chống virus cho tin nhắn**.
4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Thiết lập Chống virus cho tin nhắn

Bạn có thể thực hiện các hành động sau để thiết lập Chống virus cho tin nhắn:

- Thiết lập phạm vi bảo vệ.

  Bạn có thể mở rộng hoặc thu hẹp phạm vi bảo vệ bằng cách sửa đổi loại tin nhắn của ứng dụng nhắn tin nhanh sẽ được quét.
- Thiết lập Chống virus cho tin nhắn để đối chiếu liên kết trong các tin nhắn của ứng dụng nhắn tin nhanh với cơ sở dữ liệu các địa chỉ web độc hại và lừa đảo.

Tạo phạm vi bảo vệ của Chống virus cho tin nhắn

Phạm vi bảo vệ nói đến các đối tượng được thành phần quét khi bật. Phạm vi bảo vệ của các thành phần khác nhau có các thuộc tính khác nhau. Loại tin nhắn của ứng dụng nhắn tin nhanh được quét, cả được nhận và được gửi, đều là thuộc tính của phạm vi bảo vệ Chống virus cho tin nhắn. Theo mặc định, Chống virus cho tin nhắn sẽ quét cả tin nhắn đến và đi. Bạn có thể tắt tính năng quét lưu lượng đi.

Để tạo phạm vi bảo vệ:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Chống virus cho tin nhắn**.

   Ở phần bên phải của cửa sổ, cấu hình của thành phần Chống virus cho tin nhắn sẽ được hiển thị.
3. Trong mục **Phạm vi bảo vệ**, thực hiện một trong các thao tác sau:
   - Nếu bạn muốn Chống virus cho tin nhắn quét tất cả các tin nhắn đến và đi của ứng dụng nhắn tin nhanh, chọn **Tin nhắn gửi đến và gửi đi**.
   - Nếu bạn muốn Chống virus cho tin nhắn chỉ quét các tin nhắn đến của ứng dụng nhắn tin nhanh, chọn **Chỉ tin nhắn gửi đến**.
4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Đối chiếu các URL với cơ sở dữ liệu các URL lừa đảo và độc hại sử dụng Chống virus cho tin nhắn

Để thiết lập Chống virus cho tin nhắn cho việc đối chiếu các URL với cơ sở dữ liệu các địa chỉ web lừa đảo và độc hại:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Chống virus cho tin nhắn**.

   Ở phần bên phải của cửa sổ, cấu hình của thành phần Chống virus cho tin nhắn sẽ được hiển thị.
3. Trong khu vực **Phương thức quét**, chọn các phương thức mà bạn muốn Chống virus cho tin nhắn sử dụng:
   - Nếu bạn muốn kiểm tra các liên kết trong tin nhắn của ứng dụng nhắn tin nhanh với cơ sở dữ liệu các địa chỉ web độc hại, chọn hộp kiểm **Kiểm tra xem các liên kết có được liệt kê trong cơ sở dữ liệu các liên kết độc hại hay không**.
   - Nếu bạn muốn kiểm tra các liên kết trong tin nhắn của ứng dụng nhắn tin nhanh với cơ sở dữ liệu các địa chỉ web lừa đảo, chọn hộp kiểm **Kiểm tra nếu liên kết được liệt kê trong cơ sở dữ liệu liên kết lừa đảo**.
4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Giám sát Hệ thống

Thành phần này có thể được sử dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Microsoft Windows cho máy trạm. Thành phần này không thể được sử dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Microsoft Windows cho máy chủ tập tin.

Phần này chứa thông tin về Giám sát Hệ thống và chỉ dẫn cách để thiết lập cấu hình thành phần.

Thông tin về Giám sát Hệ thống

Giám sát Hệ thống thu thập dữ liệu về các hành động của ứng dụng trên máy tính của bạn và chuyển thông tin này đến các thành phần khác để bảo vệ tốt hơn.

Ký hiệu dòng truyền phát hành vi

Ký hiệu Dòng Truyền phát Hành vi (BSS) có chứa các chuỗi hành động ứng dụng được Kaspersky Endpoint Security phân loại là nguy hiểm. Nếu hoạt động của ứng dụng khớp với một ký hiệu dòng truyền phát hành vi cụ thể, Kaspersky Endpoint Security sẽ thực hiện hành động được quy định. Chức năng của Kaspersky Endpoint Security dựa trên các ký hiệu dòng truyền phát hành vi cung cấp một lớp bảo vệ chủ động cho máy tính.

Theo mặc định, nếu hoạt động của ứng dụng khớp với một ký hiệu dòng truyền phát hành vi, Giám sát Hệ thống sẽ di chuyển tập tin thực thi của ứng dụng đó đến Cách ly.

Khôi phục lại các hành động đã được thực hiện bởi phần mềm độc hại

Dựa trên thông tin mà Giám sát Hệ thống thu thập, Kaspersky Endpoint Security có thể **khôi phục lại các hành động đã được thực hiện bởi phần mềm độc hại trong hệ điều hành** trong quá trình khử nhiễm.

Khi khôi phục lại các hoạt động của phần mềm độc hại trong hệ điều hành, Kaspersky Endpoint Security sẽ xử lý các loại hoạt động của phần mềm độc hại sau đây:

- Hoạt động trên tập tin.

  Kaspersky Endpoint Security sẽ xóa các tập tin thực thi đã được tạo bởi chương trình độc hại và được đặt trên bất kỳ phương tiện nào, ngoại trừ các phương tiện mạng.

  Kaspersky Endpoint Security sẽ xóa các tập tin thực thi đã được tạo bởi một chương trình bị xâm nhập bởi chương trình độc hại.

  Kaspersky Endpoint Security sẽ không khôi phục các tập tin đã bị thay đổi hoặc xóa.

- Hoạt động registry.

  Kaspersky Endpoint Security sẽ xóa các phân vùng và khóa registry đã được tạo bởi phần mềm độc hại.

  Kaspersky Endpoint Security sẽ không khôi phục các phân vùng và khóa registry đã bị thay đổi hoặc xóa.

- Hoạt động hệ thống.

  Kaspersky Endpoint Security sẽ chấm dứt các tiến trình đã được khởi động bởi một chương trình độc hại.

  Kaspersky Endpoint Security sẽ chấm dứt các tiến trình bị xâm nhập bởi một chương trình độc hại.

  Kaspersky Endpoint Security sẽ không khôi phục các tiến trình đã bị dừng bởi một chương trình độc hại.

- Hoạt động mạng.

  Kaspersky Endpoint Security sẽ chặn hoạt động mạng của các chương trình độc hại.

  Kaspersky Endpoint Security sẽ chặn hoạt động mạng của các tiến trình bị xâm nhập bởi một chương trình độc hại.

Việc khôi phục lại các hành động của phần mềm độc hại có thể được bắt đầu bởi Chống virus cho tập tin hoặc trong quá trình quét virus.

Việc khôi phục lại hoạt động của phần mềm độc hại ảnh hưởng đến một nhóm dữ liệu rất cụ thể. Việc khôi phục lại không có ảnh hưởng xấu nào đến hệ điều hành hay tính toàn vẹn của dữ liệu máy tính.

Bật và tắt Giám sát Hệ thống

Theo mặc định, Giám sát Hệ thống sẽ được bật và chạy trong chế độ được khuyến nghị bởi Kaspersky Bạn có thể tắt Giám sát Hệ thống nếu cần thiết.

Bạn không nên tắt Giám sát Hệ thống trừ khi là tuyệt đối cần thiết, bởi điều này sẽ ảnh hưởng đến hiệu năng của các thành phần bảo vệ. Các thành phần bảo vệ có thể yêu cầu dữ liệu được thu thập bởi Giám sát Hệ thống để có thể xác định chính xác hơn một đối tượng được phát hiện.

Có hai cách để bật hoặc tắt Giám sát Hệ thống:

- Trên thẻ **Bảo vệ và Kiểm soát** của cửa sổ chính của ứng dụng
- Từ cửa sổ cấu hình ứng dụng.

*Để bật hoặc tắt Giám sát Hệ thống trên thẻ **Bảo vệ và Kiểm soát** của cửa sổ chính của ứng dụng:*

1. Mở cửa sổ chính của ứng dụng.
2. Chọn thẻ **Bảo vệ và Kiểm soát**.
3. Nhấn vào mục **Bảo vệ**.
   Mục **Bảo vệ** sẽ được mở ra.
4. Nhấn phải chuột để hiển thị menu ngữ cảnh của dòng có chứa thông tin về thành phần Giám sát Hệ thống.
   Một menu để chọn hành động đối với thành phần sẽ được mở ra.
5. Thực hiện một trong các thao tác sau:
   - Để bật Giám sát Hệ thống, chọn **Bắt đầu**.
     Biểu tượng trạng thái của thành phần , được hiển thị ở bên trái của dòng **Giám sát Hệ thống** sẽ được chuyển sang biểu tượng .
   - Để tắt Giám sát Hệ thống, chọn **Dừng**.
     Biểu tượng trạng thái của thành phần , được hiển thị ở bên trái của dòng **Giám sát Hệ thống** sẽ được chuyển sang biểu tượng .

Để bật hoặc tắt Giám sát Hệ thống từ cửa sổ cấu hình ứng dụng:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Giám sát Hệ thống**.
   Ở phần bên phải của cửa sổ, cấu hình của thành phần **Giám sát Hệ thống** sẽ được hiển thị.
3. Thực hiện một trong các thao tác sau:
   - Để bật Giám sát Hệ thống, chọn hộp kiểm **Bật Giám sát Hệ thống**.
   - Để tắt Giám sát Hệ thống, xóa hộp kiểm **Bật Giám sát Hệ thống**.
4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Thiết lập Giám sát Hệ thống

Bạn có thể thực hiện hành động sau để thiết lập Giám sát Hệ thống:

- bật hoặc tắt bảo vệ chống khai thác;
- chọn hành động trong trường hợp phát hiện hoạt động độc hại trong một chương trình;
- Bật hoặc tắt việc khôi phục lại hành động của phần mềm độc hại trong quá trình khử nhiễm.

Bật hoặc tắt bảo vệ chống khai thác

Để bật hoặc tắt bảo vệ chống mã khai thác:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Giám sát Hệ thống**.
   Ở phần bên phải của cửa sổ, cấu hình của thành phần **Giám sát Hệ thống** sẽ được hiển thị.
3. Thực hiện một trong các thao tác sau:
   - Chọn hộp kiểm **Cho phép chống khai thác lỗ hổng** nếu bạn muốn Kaspersky Endpoint Security giám sát các tập tin được sử dụng bởi những chương trình có lỗ hổng bảo mật khi chúng được khởi chạy.
     Nếu Kaspersky Endpoint Security phát hiện rằng một tập tin đang được sử dụng bởi một chương trình có lỗ hổng bảo mật không được khởi chạy bởi người sử dụng, nó sẽ có hành động tương ứng với lựa chọn của bạn trong danh sách hiện lên **Hành động khi phát hiện nguy hiểm**.
   - Chọn hộp kiểm **Cho phép chống khai thác lỗ hổng** nếu bạn muốn Kaspersky Endpoint Security giám sát các tập tin được sử dụng bởi những chương trình có lỗ hổng bảo mật khi chúng được khởi chạy.
4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Chọn hành động trong trường hợp phát hiện hoạt động độc hại trong một chương trình

Để lựa chọn hành động cần thực hiện nếu một chương trình tham gia vào một hoạt động độc hại, hãy thực hiện các bước sau:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Giám sát Hệ thống**.
   Ở phần bên phải của cửa sổ, cấu hình của thành phần **Giám sát Hệ thống** sẽ được hiển thị.
3. Trong mục **Hành động khi phát hiện nguy hiểm**, trong danh sách hiện lên **Phát hiện phần mềm độc hại đang hoạt động**, chọn hành động sau:
   - **Lựa chọn hành động tự động**.
   - **Di chuyển tập tin đến Cách ly**.
   - **Chấm dứt chương trình độc hại**.
   - **Bỏ qua**.
4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Bật và tắt việc khôi phục lại hành động của phần mềm độc hại trong quá trình khử nhiễm

Để bật hoặc tắt việc khôi phục lại hành động của phần mềm độc hại trong quá trình khử nhiễm:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Giám sát Hệ thống**.
   Ở phần bên phải của cửa sổ, cấu hình của thành phần **Giám sát Hệ thống** sẽ được hiển thị.
3. Thực hiện một trong các thao tác sau:
   - Nếu bạn muốn Kaspersky Endpoint Security khôi phục lại các hành động đã được thực hiện bởi phần mềm độc hại trong hệ điều hành trong quá trình khử nhiễm, chọn hộp kiểm **Khôi phục lại hành động của phần mềm độc hại trong khi khử mã độc**.
   - Nếu bạn muốn Kaspersky Endpoint Security bỏ qua các hành động đã được thực hiện bởi phần mềm độc hại trong hệ điều hành trong quá trình khử nhiễm, xóa hộp kiểm **Khôi phục lại hành động của phần mềm độc hại trong khi khử mã độc**.
4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Tường lửa

Phần này chứa thông tin về Tường lửa và chỉ dẫn cách để thiết lập cấu hình thành phần.

Thông tin về Tường lửa

Trong quá trình sử dụng trên mạng LAN và Internet, một máy tính sẽ có nguy cơ tiếp xúc với virus, phần mềm độc hại khác cùng nhiều cuộc tấn công khai thác lỗ hổng bảo mật trong các hệ điều hành và phần mềm.

Tường lửa bảo vệ dữ liệu cá nhân được lưu trữ trên máy tính của người dùng và chặn hầu hết các mối đe dọa khả dĩ đến hệ điều hành trong khi máy tính đang được kết nối đến Internet hoặc đến một mạng máy tính cục bộ. Tường lửa sẽ phát hiện tất cả các kết nối mạng của máy tính và cung cấp một danh sách các địa chỉ IP với chỉ báo về trạng thái của kết nối mạng mặc định.

Thành phần Tường lửa sẽ lọc mọi hoạt động mạng theo các quy tắc mạng. Việc thiết lập quy tắc mạng cho phép bạn quy định cấp độ bảo vệ máy tính mong muốn, từ chặn truy cập Internet cho tất cả các ứng dụng đến cho phép truy cập không giới hạn.

Bật hoặc tắt Tường lửa

Theo mặc định, Tường lửa sẽ được bật và hoạt động trong chế độ tối ưu. Nếu cần thiết, bạn có thể tắt Tường lửa.

Có hai cách để bật hoặc tắt thành phần này:

- Trên thẻ **Bảo vệ và Kiểm soát** của cửa sổ chính của ứng dụng
- Từ cửa sổ cấu hình ứng dụng.

Để bật hoặc tắt Tường lửa trên thẻ Bảo vệ và Kiểm soát của cửa sổ chính của ứng dụng:

1. Mở cửa sổ chính của ứng dụng.
2. Chọn thẻ **Bảo vệ và Kiểm soát**.
3. Nhấn vào mục **Bảo vệ**.
   Mục **Bảo vệ** sẽ được mở ra.
4. Nhấp chuột phải vào dòng **Tường lửa** để mở menu ngữ cảnh của hoạt động Tường lửa.
5. Thực hiện một trong các thao tác sau:
   - Để bật Tường lửa, trong menu ngữ cảnh, chọn **Bắt đầu**.
     Biểu tượng trạng thái của thành phần , được hiển thị ở bên trái của dòng **Tường lửa** sẽ được chuyển sang biểu tượng .
   - Để tắt Tường lửa, chọn **Dừng** trong menu ngữ cảnh.
     Biểu tượng trạng thái của thành phần , được hiển thị ở bên trái của dòng **Tường lửa** sẽ được chuyển sang biểu tượng .

Để bật hoặc tắt Tường lửa từ cửa sổ cấu hình ứng dụng:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn **Tường lửa**.
   Ở phần bên phải của cửa sổ, cấu hình của thành phần Tường lửa sẽ được hiển thị.
3. Thực hiện một trong các thao tác sau:
   - Để bật Tường lửa, chọn hộp kiểm **Bật Tường lửa**.
   - Để tắt Tường lửa, xóa hộp kiểm **Bật Tường lửa**.
4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Thông tin về quy tắc mạng

Quy tắc mạng là những hành động được cho phép hoặc bị chặn được thực hiện bởi Tường lửa khi phát hiện một nỗ lực kết nối mạng.

Tường lửa sẽ cung cấp tính năng bảo vệ chống lại các cuộc tấn công mạng khác nhau ở hai cấp độ: cấp độ mạng và cấp độ chương trình. Bảo vệ ở cấp độ mạng được cung cấp bằng cách áp dụng các quy tắc gói tin mạng. Bảo vệ ở cấp độ chương trình được cung cấp bằng cách áp dụng các quy tắc mà qua đó các ứng dụng đã cài đặt có thể truy cập tài nguyên mạng.

Dựa trên hai cấp độ bảo vệ của Tường lửa, bạn có thể tạo:

- *Những quy tắc cho gói tin mạng*. Các quy tắc gói tin mạng áp đặt hạn chế cho các gói tin mạng, bất kể chương trình là gì. Các quy tắc này hạn chế lưu lượng mạng vào và ra thông qua các cổng cụ thể của giao thức dữ liệu được chọn. Tường lửa sẽ quy định các quy tắc gói tin mạng nhất định theo mặc định.
- *Quy tắc mạng cho ứng dụng*. Các quy tắc mạng cho ứng dụng áp đặt hạn chế đối với hoạt động mạng của một ứng dụng cụ thể. Các quy tắc này không chỉ xét đến đặc tính của gói tin mạng, mà còn ứng dụng cụ thể tiếp nhận hoặc phát ra gói tin mạng này. Những quy tắc đó giúp bạn có thể tinh chỉnh bộ lọc hoạt động mạng: ví dụ, khi một loại kết nối mạng bị chặn cho một số ứng dụng, nhưng lại được cho phép cho các ứng dụng khác.

Các quy tắc gói tin mạng có ưu tiên cao hơn so với các quy tắc mạng cho ứng dụng. Nếu cả hai loại quy tắc gói tin mạng và quy tắc mạng cho ứng dụng đều được quy định cho cùng một loại hoạt động mạng, hoạt động mạng đó sẽ được xử lý theo quy tắc gói tin mạng.

Bạn có thể quy định một mức độ ưu tiên thực thi cho mỗi quy tắc gói tin mạng và cho mỗi quy tắc mạng cho ứng dụng.

Các quy tắc gói tin mạng có ưu tiên cao hơn so với các quy tắc mạng cho ứng dụng. Nếu cả hai loại quy tắc gói tin mạng và quy tắc mạng cho ứng dụng đều được quy định cho cùng một loại hoạt động mạng, hoạt động mạng đó sẽ được xử lý theo quy tắc gói tin mạng.

Các quy tắc mạng cho các ứng dụng hoạt động như sau: quy tắc mạng cho các ứng dụng bao gồm các quy tắc truy cập dựa trên trạng thái mạng: *công cộng*, *cục bộ* hoặc *tin tưởng*. Ví dụ: theo mặc định, các ứng dụng trong nhóm tin tưởng Giới hạn mức Cao sẽ không được phép thực hiện bất kỳ hoạt động mạng nào trong các mạng thuộc mọi trạng thái. Nếu quy tắc mạng được chỉ định cho một ứng dụng riêng lẻ (ứng dụng cha), thì các tiến trình con của các ứng dụng khác sẽ chạy theo quy tắc mạng của ứng dụng cha. Nếu không có quy tắc mạng cho ứng dụng, các tiến trình con sẽ chạy theo quy tắc truy cập mạng của nhóm tin tưởng của ứng dụng.

Ví dụ: bạn đã cấm mọi hoạt động mạng trong các mạng có mọi trạng thái cho tất cả các ứng dụng, ngoại trừ trình duyệt X. Nếu bạn tiến hanh cài đặt trình duyệt Y (tiến trình con) từ trình duyệt X (ứng dụng cha) thì bộ cài đặt trình duyệt Y sẽ truy cập mạng và tải xuống các tập tin cần thiết. Sau khi cài đặt, trình duyệt Y sẽ bị từ chối mọi kết nối mạng theo thiết lập Tường lửa. Để cấm hoạt động mạng của bộ cài đặt trình duyệt Y dưới dạng tiến trình con, bạn phải thêm quy tắc mạng cho bộ cài đặt trình duyệt Y.

Thông tin về trạng thái kết nối mạng

Tường lửa kiểm soát tất cả các kết nối mạng trên máy tính của người dùng và tự động gán một trạng thái cho mỗi kết nối mạng được phát hiện.

Kết nối mạng này có thể có các kiểu trạng thái sau:

- **Mạng công cộng**. Trạng thái này được áp dụng cho các mạng không được bảo vệ bởi bất kỳ ứng dụng chống virus, tường lửa hoặc bộ lọc nào (ví dụ, mạng ở các quán Internet cafe). Khi người sử dụng dùng một máy tính được kết nối đến mạng này, Tường lửa sẽ chặn truy cập đến các tập tin và máy in của máy tính. Những người dùng bên ngoài sẽ không thể truy cập dữ liệu thông qua các thư mục chia sẻ và truy cập từ xa đến màn hình làm việc của máy tính này. Tường lửa sẽ lọc các hoạt động mạng của mỗi ứng dụng theo các quy tắc mạng đã được thiết lập cho nó.

  Tường lửa sẽ gán trạng thái *Mạng công cộng* cho Internet ở chế độ mặc định. Bạn không thể thay đổi trạng thái của Internet.

- **Mạng nội bộ**. Trạng thái này được gán cho các mạng mà ở đó người dùng được tin tưởng và có thể truy cập các tập tin và máy in trên máy tính này (ví dụ, một mạng LAN hoặc mạng gia đình).

- **Mạng tin tưởng**. Trạng thái này dành cho một mạng an toàn trong đó máy tính không bị nguy cơ tấn công hay truy cập dữ liệu trái phép. Tường lửa cho phép mọi hoạt động mạng trong các mạng có trạng thái này.

Thay đổi trạng thái kết nối mạng

Để thay đổi trạng thái kết nối mạng:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Tường lửa**.

   Ở phần bên phải của cửa sổ, cấu hình của thành phần Tường lửa sẽ được hiển thị.
3. Nhấn nút **Mạng sẵn có**.

   Cửa sổ **Tường lửa** sẽ được mở ra.
4. Chọn kết nối mạng mà bạn muốn thay đổi trạng thái.
5. Trong menu ngữ cảnh, chọn trạng thái kết nối mạng:

- **Mạng công cộng**.
- **Mạng nội bộ**.
- **Mạng tin tưởng**.

6. Trong cửa sổ **Tường lửa**, nhấn **OK**.
7. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Quản lý các quy tắc gói tin mạng

Bạn có thể thực hiện các hành động sau khi quản lý các quy tắc gói tin mạng:

- Tạo một quy tắc gói tin mạng mới.

  Bạn có thể tạo một quy tắc gói tin mạng mới bằng cách tạo một nhóm các điều kiện và hành động được áp dụng đến các gói tin mạng và dòng dữ liệu.

- Bật hoặc tắt một quy tắc gói tin mạng.

  Tất cả các quy tắc gói tin mạng được tạo bởi Tường lửa theo mặc định đều có trạng thái *Bật*. Khi một quy tắc gói tin mạng được bật, Tường lửa sẽ áp dụng quy tắc này.

  Bạn có thể tắt bất kỳ quy tắc gói tin mạng nào được lựa chọn trong danh sách quy tắc gói tin mạng. Khi một quy tắc gói tin mạng bị tắt, Tường lửa sẽ tạm thời không áp dụng quy tắc mạng này.

  > Một quy tắc gói tin mạng tùy chỉnh mới sẽ được bổ sung vào danh sách các quy tắc gói tin mạng theo mặc định với trạng thái *Bật*.

- Sửa cấu hình của một quy tắc gói tin mạng hiện có.

  Sau khi bạn đã tạo một quy tắc gói tin mạng mới, bạn luôn có thể quay lại và sửa cấu hình của nó khi cần.

- Thay đổi hành động của Tường lửa cho một quy tắc gói tin mạng.

  Trong danh sách quy tắc gói tin mạng, bạn có thể sửa hành động được thực hiện bởi Tường lửa khi phát hiện các hoạt động mạng khớp với một quy tắc gói tin mạng cụ thể.

- Thay đổi mức độ ưu tiên của một quy tắc gói tin mạng.

  Bạn có thể tăng hoặc giảm mức độ ưu tiên của một quy tắc gói tin mạng được lựa chọn trong danh sách.

- Xóa một quy tắc gói tin mạng.

  Bạn có thể xóa một quy tắc gói tin mạng để Tường lửa không áp dụng quy tắc này khi phát hiện các hoạt động mạng, và để quy tắc này không được hiển thị trong danh sách các quy tắc gói tin mạng với trạng thái *Tắt*.

Tạo và sửa một quy tắc gói tin mạng

Khi tạo các quy tắc gói tin mạng, hãy nhớ rằng chúng được ưu tiên hơn các quy tắc mạng cho ứng dụng.

Để tạo hoặc sửa một quy tắc gói tin mạng:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn **Tường lửa**.
3. Nhấn nút **Những quy tắc cho gói tin mạng**.
4. Cửa sổ **Tường lửa** sẽ được mở ra thẻ **Những quy tắc cho gói tin mạng**.
   Thẻ này hiển thị một danh sách các quy tắc gói tin mạng được đặt bởi Tường lửa.
5. Thực hiện một trong các thao tác sau:
   - Để tạo một quy tắc gói tin mạng mới, nhấn nút **Thêm**.
   - Để sửa một quy tắc gói tin mạng, chọn nó trong danh sách các quy tắc gói tin mạng và nhấn nút **Chỉnh sửa**.

   Cửa sổ **Quy tắc mạng** mở ra.
6. Trong danh sách thả xuống **Hành động**, chọn hành động được thực hiện bởi Tường lửa khi phát hiện loại hoạt động mạng này:
   - **Cho phép**
   - **Ngăn chặn**
   - **Bởi các quy tắc cho ứng dụng**.
7. Trong trường **Tên**, nhập tên của dịch vụ mạng bằng một trong các cách sau:
   - Nhấn vào biểu tượng ở phía bên phải của trường **Tên** và chọn tên của dịch vụ mạng trong danh sách thả xuống.
     Các đề mục trong danh sách thả xuống bao gồm các dịch vụ mạng quy định những kết nối mạng thường được sử dụng nhất.
   - Nhập thủ công tên của dịch vụ mạng vào trường **Tên**.
8. Quy định giao thức truyền dữ liệu:
   a. Chọn hộp kiểm **Giao thức**.
   b. Trong danh sách thả xuống, chọn loại giao thức sẽ được giám sát hoạt động mạng.
      Tường lửa sẽ giám sát các kết nối mạng sử dụng các giao thức TCP, UDP, ICMP, ICMPv6, IGMP, và GRE.
      Nếu bạn lựa chọn một dịch vụ mạng từ danh sách thả xuống **Tên**, hộp kiểm **Giao thức** sẽ được chọn tự động và danh sách thả xuống cạnh hộp kiểm sẽ chứa loại giao thức tương ứng với dịch vụ mạng được lựa chọn. Hộp kiểm **Giao thức** được xóa ở chế độ mặc định.
9. Trong danh sách thả xuống **Hướng**, chọn hướng của hoạt động mạng được giám sát.

Tường lửa sẽ giám sát kết nối mạng với các hướng sau:

- **Gói tin vào (gói)**.
- **Gói tin vào**.
- **Gói tin vào / Gói tin ra**
- **Gói tin ra (gói)**.
- **Gói tin ra**.

10. Nếu ICMP hoặc ICMPv6 được lựa chọn làm giao thức, bạn có thể quy định loại gói tin và mã ICMP:

    a. Chọn hộp kiểm **Loại ICMP** và chọn loại gói tin ICMP trong danh sách thả xuống.

    b. Chọn hộp kiểm **Mã ICMP** và chọn mã gói tin ICMP trong danh sách thả xuống.

11. Nếu TCP hoặc UDP được lựa chọn làm loại giao thức, bạn có thể quy định các số hiệu cổng (được tách ra bởi dấu phẩy) của các máy tính cục bộ và từ xa mà kết nối giữa chúng được giám sát:

    a. Nhập cổng của máy tính từ xa trong trường **Cổng điều khiển từ xa**.

    b. Nhập cổng của máy tính cục bộ trong trường **Cổng cục bộ**.

12. Trong bảng **Bộ điều hợp mạng**, nhập cấu hình của bộ điều hợp mạng có thể nhận các gói tin mạng, hoặc từ đó gói tin mạng có thể được gửi đi. Để làm điều này, sử dụng các nút **Thêm**, **Chỉnh sửa**, và **Gỡ bỏ**.

13. Nếu bạn muốn hạn chế kiểm soát các gói tin mạng dựa trên thời gian sống (TTL) của chúng, chọn hộp kiểm **TTL** và trong trường cạnh nó, quy định khoảng giá trị thời gian sống cho các gói tin mạng vào và/hoặc ra.

    Một quy tắc mạng sẽ kiểm soát việc truyền tải các gói tin mạng có thời gian sống không vượt quá giá trị được quy định.

    Nếu không, hãy xóa hộp kiểm **TTL**.

14. Quy định địa chỉ mạng của các máy tính từ xa có thể gửi và / hoặc nhận gói tin mạng. Để làm điều này, chọn một trong các giá trị sau trong danh sách thả xuống **Địa chỉ từ xa**:

    - **Bất kỳ địa chỉ nào**. Quy tắc mạng sẽ kiểm soát các gói tin mạng được gửi và / hoặc được nhận bởi máy tính từ xa có bất kỳ địa chỉ IP nào.
    - **Địa chỉ mạng con**. Quy tắc mạng sẽ kiểm soát các gói tin mạng được gửi và / hoặc được nhận bởi máy tính từ xa có địa chỉ IP liên quan đến kiểu mạng được chọn: **Mạng tin tưởng**, **Mạng nội bộ**, hoặc **Mạng công cộng**.
    - **Địa chỉ từ danh sách**. Quy tắc mạng sẽ kiểm soát các gói tin mạng được gửi và / hoặc được nhận bởi máy tính từ xa có địa chỉ IP có thể được quy định trong danh sách dưới đây sử dụng các nút **Thêm**, **Chỉnh sửa** và **Gỡ bỏ**.

15. Quy định địa chỉ mạng của các máy tính cài đặt Kaspersky Endpoint Security và có thể gửi và / hoặc nhận gói tin mạng. Để làm điều này, chọn một trong các giá trị sau trong danh sách thả xuống **Địa chỉ nội bộ**:

    - **Bất kỳ địa chỉ nào**. Quy tắc mạng sẽ kiểm soát các gói tin mạng được gửi và / hoặc được nhận bởi máy tính cài đặt Kaspersky Endpoint Security và có bất kỳ địa chỉ IP nào.

- **Địa chỉ từ danh sách**. Quy tắc mạng sẽ kiểm soát các gói tin mạng được gửi và / hoặc được nhận bởi máy tính cài đặt Kaspersky Endpoint Security và có địa chỉ IP có thể được quy định trong danh sách dưới đây sử dụng các nút **Thêm**, **Chỉnh sửa** và **Gỡ bỏ**.

Đôi khi địa chỉ nội bộ không thể được lấy cho các ứng dụng làm việc với gói tin mạng. Trong trường hợp này, giá trị của cấu hình **Địa chỉ nội bộ** sẽ bị bỏ qua.

16. Nếu bạn muốn hành động của quy tắc mạng được phản ánh trong báo cáo, hãy chọn hộp kiểm **Báo cáo sự kiện**.

17. Trong cửa sổ **Quy tắc mạng**, nhấn **OK**.

    Nếu bạn tạo một quy tắc mạng mới, quy tắc này sẽ được hiển thị trong thẻ **Những quy tắc cho gói tin mạng** của cửa sổ **Tường lửa**. Theo mặc định, gói tin mạng mới sẽ được đặt ở cuối danh sách quy tắc gói tin mạng.

18. Trong cửa sổ **Tường lửa**, nhấn **OK**.

19. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Bật hoặc tắt một quy tắc gói tin mạng

Để bật hoặc tắt một quy tắc gói tin mạng:

1. Mở cửa sổ cấu hình ứng dụng.

2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Tường lửa**.

   Ở phần bên phải của cửa sổ, cấu hình của thành phần Tường lửa sẽ được hiển thị.

3. Nhấn nút **Những quy tắc cho gói tin mạng**.

   Cửa sổ **Tường lửa** sẽ được mở ra thẻ **Những quy tắc cho gói tin mạng**.

4. Chọn quy tắc gói tin mạng cần thiết trong danh sách.

5. Thực hiện một trong các thao tác sau:

   - Để bật quy tắc, chọn hộp kiểm cạnh tên của quy tắc gói tin mạng đó.
   - Để tắt quy tắc, xóa hộp kiểm cạnh tên của quy tắc gói tin mạng đó.

6. Nhấn **OK**.

7. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Thay đổi hành động của Tường lửa cho một quy tắc gói tin mạng

Để thay đổi hành động của Tường lửa cho một quy tắc gói tin mạng:

1. Mở cửa sổ cấu hình ứng dụng.

2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Tường lửa**.
   Ở phần bên phải của cửa sổ, cấu hình của thành phần Tường lửa sẽ được hiển thị.

3. Nhấn nút **Những quy tắc cho gói tin mạng**.
   Cửa sổ **Tường lửa** sẽ được mở ra thẻ **Những quy tắc cho gói tin mạng**.

4. Trong danh sách, chọn quy tắc gói tin mạng có hành động mà bạn muốn thay đổi.

5. Trong cột **Quyền**, nhấn phải chuột để gọi menu ngữ cảnh và chọn hành động mà bạn muốn gán:

   - **Cho phép**
   - **Ngăn chặn**
   - **Theo quy tắc ứng dụng**
   - **Báo cáo sự kiện**

6. Trong cửa sổ **Tường lửa**, nhấn **OK**.

7. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Thay đổi mức độ ưu tiên của một quy tắc gói tin mạng

Mức độ ưu tiên của một quy tắc gói tin mạng được quyết định bởi vị trí của nó trong danh sách các quy tắc gói tin mạng. Những quy tắc cho gói tin mạng cao nhất trong danh sách quy tắc gói tin mạng sẽ có ưu tiên cao nhất.

Các quy tắc gói tin mạng được tạo thủ công sẽ được thêm vào cuối danh sách các quy tắc gói tin mạng và có mức ưu tiên thấp nhất.

Tường lửa thực thi các quy tắc theo thứ tự xuất hiện trong danh sách quy tắc gói tin mạng, từ trên xuống dưới. Theo mỗi quy tắc gói tin mạng được xử lý áp dụng cho một kết nối mạng cụ thể, Tường lửa sẽ cho phép hoặc chặn truy cập mạng đến địa chỉ và cổng được ghi trong cấu hình của kết nối mạng này.

Để thay đổi mức độ ưu tiên của quy tắc gói tin mạng:

1. Mở cửa sổ cấu hình ứng dụng.

2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Tường lửa**.
   Ở phần bên phải của cửa sổ, cấu hình của thành phần Tường lửa sẽ được hiển thị.

3. Nhấn nút **Những quy tắc cho gói tin mạng**.
   Cửa sổ **Tường lửa** sẽ được mở ra thẻ **Những quy tắc cho gói tin mạng**.

4. Trong danh sách, chọn quy tắc gói tin mạng có mức độ ưu tiên mà bạn muốn thay đổi.

5. Sử dụng các nút **Di chuyển lên** và **Di chuyển xuống** để di chuyển quy tắc gói tin mạng đó đến vị trí mong muốn trong danh sách các quy tắc gói tin mạng.

6. Nhấn **OK**.

7. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Quản lý các quy tắc mạng cho ứng dụng

Theo mặc định, Kaspersky Endpoint Security sẽ ghép nhóm tất cả các ứng dụng được cài đặt trên máy tính theo tên của nhà cung cấp phần mềm có hoạt động tập tin hoặc mạng được ứng dụng giám sát. Các nhóm ứng dụng sẽ được phân thành các nhóm tin tưởng. Tất cả các ứng dụng và nhóm ứng dụng đều thừa hưởng thuộc tính từ nhóm cha của chúng: quy tắc kiểm soát ứng dụng, quy tắc mạng cho ứng dụng và ưu tiên thực thi.

Theo mặc định, thành phần Tường lửa sẽ áp dụng các quy tắc mạng cho một nhóm ứng dụng khi lọc hoạt động mạng của tất cả các ứng dụng trong nhóm này, tương tự như thành phần Kiểm soát Đặc quyền Ứng dụng. Quy tắc mạng cho nhóm ứng dụng quy định quyền của các ứng dụng trong nhóm trong việc truy cập các kết nối mạng khác nhau.

Theo mặc định, Tường lửa sẽ tạo một nhóm quy tắc mạng cho mỗi nhóm ứng dụng được phát hiện bởi Kaspersky Endpoint Security trên máy tính. Bạn có thể thay đổi hành động của Tường lửa được áp dụng cho các quy tắc mạng của nhóm ứng dụng được tạo theo mặc định. Bạn không thể sửa, xóa, tắt hay thay đổi mức độ ưu tiên của các quy tắc mạng cho nhóm ứng dụng được tạo theo mặc định.

Bạn cũng có thể tạo một quy tắc mạng cho từng ứng dụng riêng biệt. Quy tắc mạng đó sẽ có mức ưu tiên cao hơn quy tắc mạng của cả nhóm chứa ứng dụng đó.

Bạn có thể thực hiện các hành động khi quản lý các quy tắc mạng của ứng dụng:

- Tạo một quy tắc mạng mới.

  Bạn có thể tạo một quy tắc mạng mới cho Tường lửa sử dụng để điều tiết các hoạt động mạng của ứng dụng hoặc các ứng dụng thuộc nhóm ứng dụng được chọn.

- Bật hoặc tắt một quy tắc mạng.

  Tất cả các quy tắc mạng đều được thêm vào danh sách các quy tắc mạng của ứng dụng với trạng thái *Bật*. Nếu một quy tắc mạng được bật, Tường lửa sẽ áp dụng quy tắc đó.

  Bạn có thể tắt một quy tắc mạng được tạo thủ công. Nếu quy tắc mạng này bị tắt, Tường lửa sẽ tạm thời không áp dụng quy tắc mạng này.

- Thay đổi cấu hình của một quy tắc mạng.

  Sau khi bạn đã tạo một quy tắc mạng mới, bạn luôn có thể quay lại cấu hình và sửa cấu hình của nó khi cần.

- Thay đổi hành động của Tường lửa cho một quy tắc mạng.

  Trong danh sách các quy tắc mạng, bạn có thể sửa hành động được Tường lửa áp dụng cho quy tắc mạng khi phát hiện các hoạt động mạng trong ứng dụng hoặc nhóm ứng dụng này.

- Thay đổi mức độ ưu tiên của một quy tắc mạng.

  Bạn có thể tăng hoặc giảm mức độ ưu tiên của một quy tắc mạng tùy chỉnh.

- Xóa một quy tắc mạng.

  Bạn có thể xóa một quy tắc mạng tùy chỉnh để Tường lửa không áp dụng quy tắc mạng này đến ứng dụng hoặc nhóm ứng dụng được chọn khi phát hiện các hoạt động mạng, và để quy tắc này không được hiển thị trong danh sách các quy tắc mạng cho ứng dụng.

Tạo và sửa một quy tắc mạng cho ứng dụng

Để tạo hoặc sửa một quy tắc mạng cho một nhóm ứng dụng:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Tường lửa**.
3. Nhấn nút **Quy tắc mạng cho ứng dụng**.

   Cửa sổ **Tường lửa** sẽ được mở ra thẻ **Quy tắc quản lý ứng dụng**.
4. Trong danh sách ứng dụng, chọn ứng dụng hoặc nhóm ứng dụng mà bạn muốn cho tạo hoặc sửa một quy tắc mạng.
5. Nhấn phải chuột để gọi menu ngữ cảnh và chọn **Quy tắc ứng dụng** hoặc **Quy tắc nhóm** tùy thuộc vào việc bạn cần làm.

   Nút này mở ra cửa sổ **Quy tắc quản lý ứng dụng** hoặc **Quy tắc kiểm soát nhóm ứng dụng**.
6. Trong cửa sổ được mở ra, chọn thẻ **Quy tắc mạng**.
7. Thực hiện một trong các thao tác sau:

   - Để tạo một quy tắc mạng mới, nhấn nút **Thêm**.
   - Để sửa một quy tắc mạng, chọn nó trong danh sách các quy tắc mạng và nhấn nút **Chỉnh sửa**.

   Cửa sổ **Quy tắc mạng** mở ra.
8. Trong danh sách thả xuống **Hành động**, chọn hành động được thực hiện bởi Tường lửa khi phát hiện loại hoạt động mạng này:

   - **Cho phép**
   - **Ngăn chặn**
9. Trong trường **Tên**, nhập tên của dịch vụ mạng bằng một trong các cách sau:

   - Nhấn vào biểu tượng ở phía bên phải của trường **Tên** và chọn tên của dịch vụ mạng trong danh sách thả xuống.

     Các đề mục trong danh sách thả xuống bao gồm các dịch vụ mạng quy định những kết nối mạng thường được sử dụng nhất.
   - Nhập thủ công tên của dịch vụ mạng vào trường **Tên**.
10. Quy định giao thức truyền dữ liệu:

    a. Chọn hộp kiểm **Giao thức**.

    b. Trong danh sách thả xuống, chọn loại giao thức sẽ được giám sát hoạt động mạng.

Tường lửa sẽ giám sát các kết nối mạng sử dụng các giao thức TCP, UDP, ICMP, ICMPv6, IGMP, và GRE.

Nếu bạn lựa chọn một dịch vụ mạng từ danh sách thả xuống **Tên**, hộp kiểm **Giao thức** sẽ được chọn tự động và danh sách thả xuống cạnh hộp kiểm sẽ chứa loại giao thức tương ứng với dịch vụ mạng được lựa chọn. Hộp kiểm **Giao thức** được xóa ở chế độ mặc định.

I1. Trong danh sách thả xuống **Hướng**, chọn hướng của hoạt động mạng được giám sát.

Tường lửa sẽ giám sát kết nối mạng với các hướng sau:

- **Gói tin vào**.
- **Gói tin vào / Gói tin ra**.
- **Gói tin ra**.

I2. Nếu ICMP hoặc ICMPv6 được lựa chọn làm giao thức, bạn có thể quy định loại gói tin và mã ICMP:

a. Chọn hộp kiểm **Loại ICMP** và chọn loại gói tin ICMP trong danh sách thả xuống.

b. Chọn hộp kiểm **Mã ICMP** và chọn mã gói tin ICMP trong danh sách thả xuống.

I3. Nếu TCP hoặc UDP được lựa chọn làm loại giao thức, bạn có thể quy định các số hiệu cổng (được tách ra bởi dấu phẩy) của các máy tính cục bộ và từ xa mà kết nối giữa chúng được giám sát:

a. Nhập cổng của máy tính từ xa trong trường **Cổng điều khiển từ xa**.

b. Nhập cổng của máy tính cục bộ trong trường **Cổng cục bộ**.

I4. Quy định địa chỉ mạng của các máy tính từ xa có thể gửi và / hoặc nhận gói tin mạng. Để làm điều này, chọn một trong các giá trị sau trong danh sách thả xuống **Địa chỉ từ xa**:

- **Bất kỳ địa chỉ nào**. Quy tắc mạng sẽ kiểm soát các gói tin mạng được gửi và / hoặc được nhận bởi máy tính từ xa có bất kỳ địa chỉ IP nào.
- **Địa chỉ mạng con**. Quy tắc mạng sẽ kiểm soát các gói tin mạng được gửi và / hoặc được nhận bởi máy tính từ xa có địa chỉ IP liên quan đến kiểu mạng được chọn: **Mạng tin tưởng**, **Mạng nội bộ**, hoặc **Mạng công cộng**.
- **Địa chỉ từ danh sách**. Quy tắc mạng sẽ kiểm soát các gói tin mạng được gửi và / hoặc được nhận bởi máy tính từ xa có địa chỉ IP có thể được quy định trong danh sách dưới đây sử dụng các nút **Thêm**, **Chỉnh sửa** và **Gỡ bỏ**.

I5. Quy định địa chỉ mạng của các máy tính cài đặt Kaspersky Endpoint Security và có thể gửi và / hoặc nhận gói tin mạng. Để làm điều này, chọn một trong các giá trị sau trong danh sách thả xuống **Địa chỉ nội bộ**:

- **Bất kỳ địa chỉ nào**. Quy tắc mạng sẽ kiểm soát các gói tin mạng được gửi và / hoặc được nhận bởi máy tính cài đặt Kaspersky Endpoint Security và có bất kỳ địa chỉ IP nào.
- **Địa chỉ từ danh sách**. Quy tắc mạng sẽ kiểm soát các gói tin mạng được gửi và / hoặc được nhận bởi máy tính cài đặt Kaspersky Endpoint Security và có địa chỉ IP có thể được quy định trong danh sách dưới đây sử dụng các nút **Thêm**, **Chỉnh sửa** và **Gỡ bỏ**.

Đôi khi địa chỉ nội bộ không thể được lấy cho các ứng dụng làm việc với gói tin mạng. Trong trường hợp này, giá trị của cấu hình **Địa chỉ nội bộ** sẽ bị bỏ qua.

16. Nếu bạn muốn hành động của quy tắc mạng được phản ánh trong báo cáo, hãy chọn hộp kiểm **Báo cáo sự kiện**.

17. Trong cửa sổ **Quy tắc mạng**, nhấn **OK**.

    Nếu bạn đã tạo một quy tắc mạng mới, quy tắc này sẽ được hiển thị trên thẻ **Quy tắc mạng**.

18. Nhấn **OK** trong cửa sổ **Quy tắc kiểm soát nhóm ứng dụng** nếu quy tắc này được dành cho một nhóm ứng dụng, hoặc trong cửa sổ **Quy tắc quản lý ứng dụng** nếu quy tắc này được dành cho một ứng dụng.

19. Trong cửa sổ **Tường lửa**, nhấn **OK**.

20. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Bật và tắt một quy tắc mạng cho ứng dụng

Để bật hoặc tắt một quy tắc mạng cho ứng dụng:

1. Mở cửa sổ cấu hình ứng dụng.

2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Tường lửa**.

   Ở phần bên phải của cửa sổ, cấu hình của thành phần Tường lửa sẽ được hiển thị.

3. Nhấn nút **Quy tắc mạng cho ứng dụng**.

   Cửa sổ **Tường lửa** sẽ được mở ra thẻ **Quy tắc quản lý ứng dụng**.

4. Trong danh sách ứng dụng, chọn ứng dụng hoặc nhóm ứng dụng mà bạn muốn bật hoặc tắt một quy tắc mạng.

5. Nhấn phải chuột để gọi menu ngữ cảnh và chọn **Quy tắc ứng dụng** hoặc **Quy tắc nhóm** tùy thuộc vào việc bạn cần làm.

   Nút này mở ra cửa sổ **Quy tắc quản lý ứng dụng** hoặc **Quy tắc kiểm soát nhóm ứng dụng**.

6. Trong cửa sổ được mở ra, chọn thẻ **Quy tắc mạng**.

7. Trong danh sách các quy tắc mạng cho một nhóm ứng dụng, chọn quy tắc mạng liên quan.

8. Thực hiện một trong các thao tác sau:

   - Nếu bạn muốn bật quy tắc, chọn hộp kiểm cạnh tên của quy tắc mạng đó.
   - Nếu bạn muốn tắt quy tắc, xóa hộp kiểm cạnh tên của quy tắc mạng đó.

   > Bạn không thể tắt một quy tắc mạng cho nhóm ứng dụng được tạo bởi Tường lửa ở chế độ mặc định.

9. Nhấn **OK** trong cửa sổ **Quy tắc kiểm soát nhóm ứng dụng** nếu quy tắc này được dành cho một nhóm ứng dụng, hoặc trong cửa sổ **Quy tắc quản lý ứng dụng** nếu quy tắc này được dành cho một ứng dụng.

10. Trong cửa sổ **Tường lửa**, nhấn **OK**.

11. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Thay đổi hành động của Tường lửa cho một quy tắc mạng cho ứng dụng

Bạn có thể thay đổi hành động của Tường lửa được áp dụng cho tất cả các quy tắc mạng của một ứng dụng hoặc nhóm ứng dụng được tạo theo mặc định, và thay đổi hành động của Tường lửa cho một quy tắc mạng tùy chỉnh cho một ứng dụng hoặc nhóm ứng dụng.

Để thay đổi hành động của Tường lửa cho tất cả các quy tắc mạng cho một ứng dụng hoặc nhóm ứng dụng:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Tường lửa**.
   Ở phần bên phải của cửa sổ, cấu hình của thành phần Tường lửa sẽ được hiển thị.
3. Nhấn nút **Quy tắc mạng cho ứng dụng**.
   Cửa sổ **Tường lửa** sẽ được mở ra thẻ **Quy tắc quản lý ứng dụng**.
4. Nếu bạn muốn thay đổi hành động của Tường lửa được áp dụng cho các quy tắc mạng được tạo theo mặc định, chọn một ứng dụng hoặc nhóm ứng dụng trong danh sách. Các quy tắc mạng được tạo thủ công sẽ được giữ nguyên.
5. Trong cột **Mạng**, nhấn để hiển thị menu ngữ cảnh và chọn hành động mà bạn muốn gán:
   - **Kế thừa**
   - **Cho phép**
   - **Ngăn chặn**
6. Nhấn **OK**.
7. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Để thay đổi phản ứng của Tường lửa cho một quy tắc mạng cho một ứng dụng hoặc nhóm ứng dụng:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn **Tường lửa**.
   Ở phần bên phải của cửa sổ, cấu hình của thành phần Tường lửa sẽ được hiển thị.
3. Nhấn nút **Quy tắc mạng cho ứng dụng**.
   Cửa sổ **Tường lửa** sẽ được mở ra thẻ **Quy tắc quản lý ứng dụng**.
4. Trong danh sách ứng dụng, chọn ứng dụng hoặc nhóm ứng dụng mà bạn muốn thay đổi hành động cho một quy tắc mạng.
5. Nhấn phải chuột để gọi menu ngữ cảnh và chọn **Quy tắc ứng dụng** hoặc **Quy tắc nhóm** tùy thuộc vào việc bạn cần làm.
   Nút này mở ra cửa sổ **Quy tắc quản lý ứng dụng** hoặc **Quy tắc kiểm soát nhóm ứng dụng**.

6. Trong cửa sổ được mở ra, chọn thẻ **Quy tắc mạng**.
7. Chọn quy tắc mạng mà bạn muốn thay đổi hành động Tường lửa.
8. Trong cột **Quyền**, nhấn phải chuột để gọi menu ngữ cảnh và chọn hành động mà bạn muốn gán:
   - **Cho phép**
   - **Ngăn chặn**
   - **Báo cáo sự kiện**
9. Nhấn **OK** trong cửa sổ **Quy tắc kiểm soát nhóm ứng dụng** nếu quy tắc này được dành cho một nhóm ứng dụng, hoặc trong cửa sổ **Quy tắc quản lý ứng dụng** nếu quy tắc này được dành cho một ứng dụng.
10. Trong cửa sổ **Tường lửa**, nhấn **OK**.
11. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Thay đổi mức độ ưu tiên của một quy tắc mạng cho ứng dụng

Mức độ ưu tiên của một quy tắc mạng được quyết định bởi vị trí của nó trong danh sách các quy tắc mạng. Tường lửa thực thi các quy tắc theo thứ tự xuất hiện trong danh sách quy tắc mạng, từ trên xuống dưới. Theo mỗi quy tắc mạng được xử lý áp dụng cho một kết nối mạng cụ thể, Tường lửa sẽ cho phép hoặc chặn truy cập mạng đến địa chỉ và cổng được ghi trong cấu hình của kết nối mạng này.

Các quy tắc mạng được tạo thủ công có mức ưu tiên cao hơn so với các quy tắc mạng mặc định.

Bạn không thể thay đổi mức độ ưu tiên của các quy tắc mạng cho nhóm ứng dụng được tạo theo mặc định.

Để thay đổi mức độ ưu tiên của một quy tắc mạng:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Tường lửa**.
   Ở phần bên phải của cửa sổ, cấu hình của thành phần Tường lửa sẽ được hiển thị.
3. Nhấn nút **Quy tắc mạng cho ứng dụng**.
   Cửa sổ **Tường lửa** sẽ được mở ra thẻ **Quy tắc quản lý ứng dụng**.
4. Trong danh sách ứng dụng, chọn ứng dụng hoặc nhóm ứng dụng mà bạn muốn thay đổi mức độ ưu tiên của quy tắc mạng.
5. Nhấn phải chuột để gọi menu ngữ cảnh và chọn **Quy tắc ứng dụng** hoặc **Quy tắc nhóm** tùy thuộc vào việc bạn cần làm.
   Nút này mở ra cửa sổ **Quy tắc quản lý ứng dụng** hoặc **Quy tắc kiểm soát nhóm ứng dụng**.
6. Trong cửa sổ được mở ra, chọn thẻ **Quy tắc mạng**.

7. Chọn quy tắc mạng có mức độ ưu tiên mà bạn muốn thay đổi.

8. Sử dụng các nút **Di chuyển lên** và **Di chuyển xuống** để di chuyển quy tắc đó đến vị trí mong muốn trong danh sách các quy tắc mạng.

9. Nhấn **OK** trong cửa sổ **Quy tắc kiểm soát nhóm ứng dụng** nếu quy tắc này được dành cho một nhóm ứng dụng, hoặc trong cửa sổ **Quy tắc quản lý ứng dụng** nếu quy tắc này được dành cho một ứng dụng.

10. Trong cửa sổ **Tường lửa**, nhấn **OK**.

11. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Giám sát mạng

Phần này chứa thông tin về Giám sát mạng và hướng dẫn cách bắt đầu Giám sát mạng.

Thông tin về Giám sát mạng

Giám sát mạng là một công cụ được thiết kế để xem thông tin về hoạt động mạng của một máy tính trong thời gian thực.

Bắt đầu Giám sát mạng

Để bắt đầu Giám sát mạng:

1. Mở cửa sổ chính của ứng dụng.

2. Chọn thẻ **Bảo vệ và Kiểm soát**.

3. Nhấn vào mục **Bảo vệ**.

   Mục **Bảo vệ** sẽ được mở ra.

4. Nhấp chuột phải vào dòng **Tường lửa** để mở menu ngữ cảnh của hoạt động Tường lửa.

5. Trong menu ngữ cảnh, chọn **Giám sát mạng**.

   Cửa sổ **Giám sát mạng** sẽ được mở ra. Trong cửa sổ này, những thông tin về hoạt động mạng của máy tính sẽ được hiển thị trên bốn thẻ:

   - Thẻ **Mạng lưới hoạt động** hiển thị tất cả các kết nối mạng đang hoạt động trên máy tính. Cả hai loại kết nối mạng vào và ra đều được hiển thị.

   - Thẻ **Mở cổng** liệt kê tất cả các cổng mạng mở của máy tính.

   - Thẻ **Lưu thông mạng** hiển thị lưu lượng mạng vào và ra giữa máy tính của người dùng và các máy tính khác trong mạng mà người dùng đang được kết nối.

   - Thẻ **Máy tính bị ngăn chặn** hiển thị các địa chỉ IP của những máy tính từ xa có hoạt động mạng bị chặn bởi thành phần Ngăn chặn Tấn công Mạng sau khi phát hiện các nỗ lực tấn công mạng từ

những địa chỉ IP đó.

Ngăn chặn tấn công mạng

Mục này chứa thông tin về Ngăn chặn tấn công mạng và chỉ dẫn cách để thiết lập cấu hình thành phần.

Thông tin về Ngăn chặn tấn công mạng

Ngăn chặn tấn công mạng sẽ quét lưu lượng mạng vào để phát hiện các hoạt động tương tự với các cuộc tấn công mạng. Khi phát hiện một nỗ lực tấn công mạng nhắm vào máy tính của bạn, Kaspersky Endpoint Security sẽ chặn hoạt động mạng từ máy tính tấn công. Khi đó, màn hình của bạn sẽ hiển thị một cảnh báo rằng một cuộc tấn công mạng đã xảy ra, và hiển thị thông tin về máy tính tấn công.

Lưu lượng mạng từ máy tính tấn công sẽ bị chặn trong một giờ. Bạn có thể sửa cấu hình được sử dụng để chặn một máy tính tấn công.

Mô tả về các hình thức tấn công mạng đã biết và các cách để chống lại chúng được cung cấp trong cơ sở dữ liệu của Kaspersky Endpoint Security. Danh sách các cuộc tấn công mạng được thành phần Ngăn chặn tấn công mạng phát hiện sẽ được cập nhật trong bản cập nhật cơ sở dữ liệu và mô-đun ứng dụng.

Bật và tắt Ngăn chặn tấn công mạng

Theo mặc định, Ngăn chặn tấn công mạng sẽ được bật và hoạt động trong chế độ tối ưu. Bạn có thể tắt Ngăn chặn tấn công mạng nếu cần thiết.

Có hai cách để bật hoặc tắt thành phần này:

- Trên thẻ **Bảo vệ và Kiểm soát** của cửa sổ chính của ứng dụng
- Từ cửa sổ cấu hình ứng dụng.

Để bật hoặc tắt Ngăn chặn tấn công mạng, thực hiện hành động sau trên thẻ Bảo vệ và Kiểm soát của cửa sổ chính của ứng dụng:

1. Mở cửa sổ chính của ứng dụng.
2. Chọn thẻ **Bảo vệ và Kiểm soát**.
3. Nhấn vào mục **Bảo vệ**.

   Mục **Bảo vệ** sẽ được mở ra.
4. Nhấn phải chuột lên dòng **Ngăn chặn tấn công mạng** để hiển thị menu ngữ cảnh của hành động Ngăn chặn tấn công mạng.
5. Thực hiện một trong các thao tác sau:

   - Để bật Ngăn chặn tấn công mạng, chọn **Bắt đầu** trong menu ngữ cảnh.

     Biểu tượng trạng thái của thành phần , được hiển thị ở bên trái của dòng **Ngăn chặn tấn công mạng** sẽ được chuyển sang biểu tượng .
   - Để tắt Ngăn chặn tấn công mạng, chọn **Dừng** trong menu ngữ cảnh.

     Biểu tượng trạng thái của thành phần , được hiển thị ở bên trái của dòng **Ngăn chặn tấn công mạng** sẽ được chuyển sang biểu tượng .

Để bật hoặc tắt Ngăn chặn tấn công mạng từ cửa sổ cấu hình ứng dụng:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Ngăn chặn tấn công mạng**.

   Cấu hình của Ngăn chặn tấn công mạng sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Làm các bước sau:
   - Để bật Ngăn chặn tấn công mạng, chọn hộp kiểm **Cho phép ngăn chặn tấn công mạng**.
   - Để tắt Ngăn chặn tấn công mạng, xóa hộp kiểm **Cho phép ngăn chặn tấn công mạng**.
4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Thiết lập Ngăn chặn Tấn công Mạng

Bạn có thể thực hiện hành động sau để thiết lập cấu hình Ngăn chặn tấn công mạng:

- Thiết lập cấu hình được sử dụng để chặn một máy tính tấn công.
- Tạo một danh sách các địa chỉ được loại trừ khỏi quy tắc chặn.

Sửa cấu hình được sử dụng để chặn một máy tính tấn công.

Để sửa cấu hình được sử dụng để chặn một máy tính tấn công:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Ngăn chặn tấn công mạng**.

   Cấu hình của Ngăn chặn tấn công mạng sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Chọn hộp kiểm **Thêm máy tính tấn công vào danh sách các máy tính bị chặn trong**.

   Nếu hộp kiểm này được chọn, khi phát hiện một nỗ lực tấn công mạng, Ngăn chặn tấn công mạng sẽ chặn lưu lượng mạng từ máy tính tấn công trong một khoảng thời gian được quy định. Điều này sẽ tự động bảo vệ chống lại các cuộc tấn công mạng có thể có trong tương lai từ cùng một địa chỉ.

   Nếu hộp kiểm này bị xóa, khi phát hiện một nỗ lực tấn công mạng, Ngăn chặn tấn công mạng sẽ không tự động bật tính năng bảo vệ chống lại các cuộc tấn công mạng có thể có trong tương lai từ cùng một địa chỉ.
4. Thay đổi khoảng thời gian trong đó một máy tính tấn công bị chặn trong trường cạnh hộp kiểm **Thêm máy tính tấn công vào danh sách các máy tính bị chặn trong**.
5. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Thiết lập các địa chỉ được loại trừ khỏi quy tắc chặn

Để thiết lập các địa chỉ được loại trừ khỏi quy tắc chặn:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Ngăn chặn tấn công mạng**.

   Cấu hình của Ngăn chặn tấn công mạng sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Nhấn nút **Loại trừ**.

   Cửa sổ **Loại trừ** sẽ được mở ra.
4. Thực hiện một trong các thao tác sau:

   - Nếu bạn muốn bổ sung một địa chỉ IP mới, nhấn nút **Thêm**.
   - Nếu bạn muốn sửa một địa chỉ IP được bổ sung từ trước, chọn nó trong danh sách các địa chỉ và nhấn nút **Sửa**.

   Cửa sổ **Địa chỉ IP** sẽ được mở ra.
5. Nhập địa chỉ IP của máy tính mà các cuộc tấn công mạng xuất phát từ đó sẽ không bị chặn.
6. Trong cửa sổ **Địa chỉ IP**, nhấn **OK**.
7. Trong cửa sổ **Loại trừ**, nhấn **OK**.
8. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Phòng chống Tấn công BadUSB

Phần này chứa thông tin về thành phần Phòng chống Tấn công BadUSB.

Thông tin về Phòng chống Tấn công BadUSB

Một số virus sẽ thay đổi firmware của các thiết bị USB để đánh lừa hệ điều hành rằng thiết bị USB đó là một bàn phím.

Thành phần Phòng chống Tấn công BadUSB sẽ ngăn các thiết bị USB bị nhiễm giả làm một bàn phím khỏi kết nối đến máy tính.

Khi một thiết bị USB được kết nối đến máy tính và được ứng dụng xác định là một bàn phím, ứng dụng sẽ nhắc người dùng nhập một mã số được tạo bởi ứng dụng từ bàn phím này, hoặc sử dụng Bàn phím Ảo (nếu khả dụng). Thủ tục này được gọi là xác thực bàn phím. Ứng dụng sẽ cho phép sử dụng một bàn phím được xác thực và chặn bàn phím không được xác thực.

Phòng chống Tấn công BadUSB sẽ chạy trong chế độ nền ngay khi thành phần này được cài đặt. Nếu ứng dụng không được áp đặt một chính sách Kaspersky Security Center, bạn có thể bật hoặc tắt Phòng chống Tấn công BadUSB bằng cách tạm ngưng và khôi phục lại tính năng bảo vệ và kiểm soát máy tính.

Cài đặt thành phần Phòng chống Tấn công BadUSB

Nếu bạn đã chọn cài đặt cơ bản hoặc tiêu chuẩn trong quá trình cài đặt Kaspersky Endpoint Security, thành phần Phòng chống Tấn công BadUSB sẽ không khả dụng. Để cài đặt nó, bạn phải thay đổi nhóm các thành phần của ứng dụng.

Để cài đặt thành phần Phòng chống Tấn công BadUSB:

1. Trong menu **Start**, chọn Applications → Kaspersky Endpoint Security 10 for Windows → **Modify, Repair, or Remove**.

   Trình hướng dẫn cài đặt sẽ được bắt đầu.

2. Trong cửa sổ **Thay đổi, Sửa chữa, hoặc Gỡ bỏ ứng dụng** của Trình hướng dẫn Cài đặt Ứng dụng, nhấn nút **Thay đổi**.

   Việc này sẽ mở ra cửa sổ **Cài đặt tùy chỉnh** của Trình hướng dẫn Cài đặt Ứng dụng.

3. Trong menu ngữ cảnh của biểu tượng cạnh tên của thành phần **Phòng chống Tấn công BadUSB**, chọn mục **Tính năng này sẽ được cài đặt trên ổ cứng của máy tính**.

4. Nhấn nút **Tiếp theo**.

5. Làm theo chỉ dẫn của Trình hướng dẫn cài đặt.

Bật và tắt Phòng chống Tấn công BadUSB

Để bật hoặc tắt Phòng chống Tấn công BadUSB:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Phòng chống Tấn công BadUSB**.

   Thiết lập Phòng chống Tấn công BadUSB sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Thực hiện một trong các thao tác sau:
   - Để bật Phòng chống Tấn công BadUSB, chọn hộp kiểm **Bật Phòng chống Tấn công BadUSB**.
   - Để tắt Phòng chống Tấn công BadUSB, bỏ chọn hộp kiểm **Bật Phòng chống Tấn công BadUSB**.
4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Cho phép và cấm sử dụng Bàn phím Ảo để xác thực

Bàn phím Ảo chỉ nên được sử dụng để xác thực các thiết bị USB không hỗ trợ việc nhập liệu ký tự ngẫu nhiên (ví dụ như đầu quét mã vạch). Bạn không nên sử dụng Bàn phím Ảo để xác thực các thiết bị USB không xác định.

Để cho phép và cấm sử dụng Bàn phím Ảo để xác thực:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảo vệ Chống virus**, chọn mục con **Phòng chống Tấn công BadUSB**.

   Cấu hình của thành phần sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Thực hiện một trong các thao tác sau:
   - Chọn hộp kiểm **Cấm sử dụng Bàn phím ảo để xác thực** để chặn việc sử dụng Bàn phím Ảo cho việc xác thực.
   - Xóa hộp kiểm **Cấm sử dụng Bàn phím ảo để xác thực** để cho phép việc sử dụng Bàn phím Ảo cho việc xác thực.
4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Xác thực bàn phím

Các thiết bị USB được hệ điều hành xác định là bàn phím và được kết nối đến máy tính trước khi cài đặt thành phần Phòng chống Tấn công BadUSB sẽ được coi là đã xác thực sau khi cài đặt thành phần.

Ứng dụng sẽ chỉ yêu cầu xác thực thiết bị USB được kết nối đã được hệ điều hành xác định là một bàn phím nếu lời nhắc xác thực bàn phím USB được bật. Người dùng không thể sử dụng một bàn phím chưa được xác thực cho đến khi nó đã được xác thực.

Nếu lời nhắc xác thực bàn phím USB bị tắt, người dùng có thể sử dụng tất cả các bàn phím được kết nối. Ngay sau khi lời nhắc xác thực bàn phím USB được bật, ứng dụng sẽ hiển thị một lời nhắc xác thực từng bàn phím chưa được xác thực được kết nối với máy.

Để xác thực một bàn phím:

1. Với tính năng xác thực bàn phím USB được bật, kết nối bàn phím đó đến một cổng USB.

   Cửa sổ **Xác thực bàn phím <tên bàn phím>** sẽ được mở ra với chi tiết về bàn phím được kết nối và một mã số để xác thực nó.

2. Nhập mã số được tạo ngẫu nhiên này vào cửa sổ xác thực từ bàn phím được kết nối hoặc Bàn phím Ảo (nếu khả dụng).

3. Nhấn **OK**.

   Nếu mã đã được nhập đúng, ứng dụng sẽ lưu lại các tham số nhận dạng – VID/PID của bàn phím và số hiệu của cổng mà nó được kết nối – trong danh sách các bàn phím được xác thực. Việc xác thực sẽ không cần được lặp lại khi bàn phím được kết nối lại hoặc sau khi hệ điều hành được khởi động lại.

   > Khi bàn phím được xác thực được kết nối đến một cổng USB khác của máy tính, ứng dụng sẽ hiển thị một lời nhắc để xác thực lại bàn phím này.

   Nếu mã số này được nhập không chính xác, ứng dụng sẽ tạo một mã mới. Bạn có thể thử nhập mã số ba lần. Nếu mã số này bị nhập sai 3 lần liên tiếp hoặc cửa sổ **Xác thực bàn phím <Tên bàn phím>** bị đóng, ứng dụng sẽ chặn dữ liệu nhập vào từ bàn phím này. Khi bàn phím được kết nối lại hoặc sau khi hệ điều hành được khởi động lại, ứng dụng sẽ nhắc người dùng thực hiện lại quy trình xác thực bàn phím.

Kiểm soát ứng dụng khởi động

Mục này chứa thông tin về Kiểm soát ứng dụng khởi động và chỉ dẫn cách để thiết lập cấu hình thành phần.

Thông tin về Kiểm soát ứng dụng khởi động

Thành phần Kiểm soát ứng dụng khởi động giám sát các nỗ lực của người dùng trong việc khởi chạy các ứng dụng và điều tiết việc khởi chạy các ứng dụng thông qua *các quy tắc Kiểm soát ứng dụng khởi động*.

Khởi động các ứng dụng có cấu hình không khớp với bất kỳ quy tắc Kiểm soát ứng dụng khởi động nào được điều tiết bởi chế độ hoạt động được chọn của thành phần. *Chế độ Danh sách Đen* được chọn theo mặc định. Chế độ này cho phép mọi người dùng có thể khởi động mọi ứng dụng.

Tất cả các nỗ lực khởi động ứng dụng của người dùng đều được ghi lại trong Báo cáo.

Bật và tắt Kiểm soát ứng dụng khởi động

Tuy Kiểm soát khởi động ứng dụng bị tắt theo mặc định, bạn có thể bật Kiểm soát khởi động ứng dụng nếu cần.

Có hai cách để bật hoặc tắt thành phần này:

- Trên thẻ **Bảo vệ và Kiểm soát** của cửa sổ chính của ứng dụng
- Từ cửa sổ cấu hình ứng dụng.

Để bật hoặc tắt Kiểm soát ứng dụng khởi động trên thẻ Bảo vệ và Kiểm soát của cửa sổ chính của ứng dụng:

1. Mở cửa sổ chính của ứng dụng.
2. Chọn thẻ **Bảo vệ và Kiểm soát**.
3. Nhấn vào mục **Bảng kiểm soát**.
   Mục **Bảng kiểm soát** sẽ được mở ra.
4. Nhấn phải chuột để gọi menu ngữ cảnh của dòng có chứa thông tin về thành phần Kiểm soát ứng dụng khởi động.
   Một menu để chọn hành động đối với thành phần sẽ được mở ra.
5. Thực hiện một trong các thao tác sau:
   - Để bật Kiểm soát ứng dụng khởi động, chọn **Bắt đầu** trong menu.
     Biểu tượng trạng thái của thành phần , được hiển thị ở bên trái của dòng **Kiểm soát ứng dụng khởi động** sẽ được chuyển sang biểu tượng .
   - Để tắt thành phần Kiểm soát ứng dụng khởi động, chọn **Dừng** trong menu.
     Biểu tượng trạng thái của thành phần , được hiển thị ở bên trái của dòng **Kiểm soát ứng dụng khởi động** sẽ được chuyển sang biểu tượng .

Để bật hoặc tắt Kiểm soát ứng dụng khởi động từ cửa sổ cấu hình ứng dụng:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát ứng dụng khởi động**.

   Cấu hình của thành phần Kiểm soát ứng dụng khởi động sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Thực hiện một trong các thao tác sau:
   - Để bật Kiểm soát ứng dụng khởi động, chọn hộp kiểm **Bật Kiểm soát ứng dụng khởi động**.
   - Để tắt Kiểm soát ứng dụng khởi động, xóa hộp kiểm **Bật Kiểm soát ứng dụng khởi động**.
4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Giới hạn chức năng của Kiểm soát ứng dụng khởi động

Hoạt động của thành phần Kiểm soát Khởi động Ứng dụng sẽ bị giới hạn trong các trường hợp sau:

- Khi phiên bản ứng dụng được nâng cấp, tác vụ nhập cấu hình của thành phần Kiểm soát Khởi động Ứng dụng sẽ không được hỗ trợ.

  Để khôi phục chức năng của Kiểm soát Khởi động Ứng dụng, bạn phải thiết lập lại cấu hình của thành phần.
- Nếu không có kết nối với máy chủ KSN, Kaspersky Endpoint Security sẽ chỉ có thể nhận thông tin về danh tiếng của các ứng dụng và mô-đun của chúng từ các cơ sở dữ liệu cục bộ. Nếu cơ sở dữ liệu cục bộ không chứa thông tin về ứng dụng, ứng dụng sẽ không được phân loại vào một nhóm tin tưởng.

  Việc phân loại các ứng dụng khi có một kết nối với máy chủ KSN có thể sẽ khác với việc phân loại chúng khi không có kết nối với KSN.
- Tại cơ sở dữ liệu Kaspersky Security Center, thông tin về 150.000 tập tin được xử lý có thể được lưu trữ. Một khi số bản ghi này đã bị vượt quá, các tập tin mới sẽ không được xử lý. Để khôi phục các thao tác kiểm kho, bạn phải xóa các tập tin đã được kiểm kho trước đây trong cơ sở dữ liệu Kaspersky Security Center khỏi máy tính có cài đặt Kaspersky Endpoint Security.
- Thành phần này không kiểm soát việc khởi động các kịch bản trừ khi kịch bản được gửi đến trình biên dịch thông qua dòng lệnh.

  Nếu việc khởi động một trình biên dịch là được cho phép bởi các quy tắc Kiểm soát Khởi động Ứng dụng, thành phần này sẽ không chặn một kịch bản được khởi chạy từ trình biên dịch này.
- Thành phần này không kiểm soát việc khởi động các kịch bản từ các trình biên dịch không được hỗ trợ bởi Kaspersky Endpoint Security.

  Kaspersky Endpoint Security hỗ trợ các trình biên dịch sau:
  - Java

- PowerShell

Các loại trình biên dịch sau không được hỗ trợ:

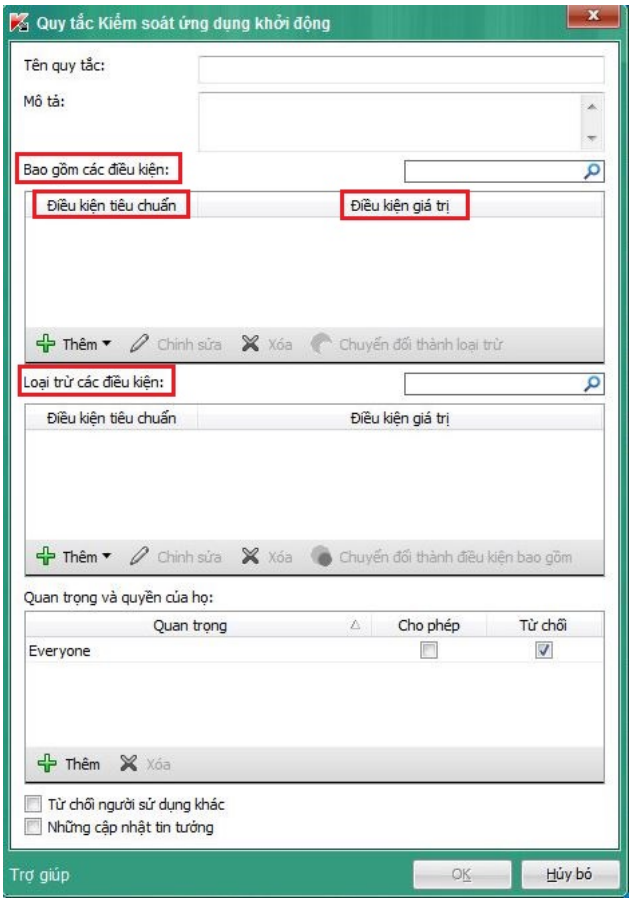
- { cCmdLineParser::itCmd, _T("%ComSpec%") };
- { cCmdLineParser::itReg, _T("%SystemRoot%\\system32\\reg.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\system32\\regedit.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\regedit.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\system32\\regedt32.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\\system32\\cscript.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\\system32\\wscript.exe") };
- { cCmdLineParser::itMsiexec, _T("%SystemRoot%\\system32\\msiexec.exe") };
- { cCmdLineParser::itMmc, _T("%SystemRoot%\\system32\\mmc.exe") };
- { cCmdLineParser::itMshta, _T("%SystemRoot%\\system32\\mshta.exe") };
- { cCmdLineParser::itRundll, _T("%SystemRoot%\\system32\\rundll32.exe") };
- { cCmdLineParser::itMetro, _T("%SystemRoot%\\system32\\wwahost.exe") };
- { cCmdLineParser::itCmd, _T("%SystemRoot%\\syswow64\\cmd.exe") };
- { cCmdLineParser::itReg, _T("%SystemRoot%\\syswow64\\reg.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\syswow64\\regedit.exe") };
- { cCmdLineParser::itRegedit, _T("%SystemRoot%\\syswow64\\regedt32.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\\syswow64\\cscript.exe") };
- { cCmdLineParser::itCWScript, _T("%SystemRoot%\\syswow64\\wscript.exe") };
- { cCmdLineParser::itMsiexec, _T("%SystemRoot%\\syswow64\\msiexec.exe") };
- { cCmdLineParser::itMmc, _T("%SystemRoot%\\syswow64\\mmc.exe") };
- { cCmdLineParser::itMshta, _T("%SystemRoot%\\syswow64\\mshta.exe") };
- { cCmdLineParser::itRundll, _T("%SystemRoot%\\syswow64\\rundll32.exe") };
- { cCmdLineParser::itMetro, _T("%SystemRoot%\\syswow64\\wwahost.exe") }.

Thông tin về quy tắc Kiểm soát ứng dụng khởi động

Kaspersky Endpoint Security kiểm soát việc khởi động của các ứng dụng người dùng bằng các quy tắc. Một quy tắc Kiểm soát ứng dụng khởi động quy định điều kiện kích hoạt và hành động được thực hiện bởi Kiểm soát ứng dụng khởi động khi quy tắc đó được kích hoạt (cho phép hoặc chặn việc khởi động ứng dụng bởi người dùng).

Điều kiện kích hoạt quy tắc

Một điều kiện kích hoạt quy tắc có các đặc điểm sau: "loại điều kiện - tiêu chí điều kiện - giá trị điều kiện" (xem hình bên dưới). Dựa vào điều kiện kích hoạt quy tắc, Kaspersky Endpoint Security cũng áp dụng (hoặc không áp dụng) một quy tắc đến cho ứng dụng.



Quy tắc Kiểm soát ứng dụng khởi động. Tham số điều kiện kích hoạt quy tắc

Các quy tắc sử dụng điều kiện bao gồm và loại trừ:

- *Điều kiện bao gồm*. Kaspersky Endpoint Security sẽ áp dụng quy tắc đến ứng dụng nếu ứng dụng khớp với ít nhất một điều kiện bao gồm.
- *Điều kiện loại trừ*. Kaspersky Endpoint Security sẽ không áp dụng quy tắc đến ứng dụng nếu ứng dụng khớp với ít nhất một điều kiện loại trừ và không khớp bất kỳ điều kiện bao gồm nào.

Điều kiện kích hoạt quy tắc được tạo sử dụng các tiêu chí. Các tiêu chí sau được sử dụng để tạo các quy tắc trong Kaspersky Endpoint Security:

- Đường dẫn đến thư mục chứa tập tin thực thi của ứng dụng hoặc đường dẫn đến tập tin thực thi của ứng dụng.
- Siêu dữ liệu: tên tập tin thực thi của ứng dụng, phiên bản tập tin thực thi của ứng dụng, tên ứng dụng, phiên bản ứng dụng, nhà cung cấp ứng dụng.

- Mã băm của tập tin thực thi của ứng dụng.
- Chứng nhận: đơn vị cấp, bên chính, vân tay.
- Tình trạng bao gồm của ứng dụng trong một hạng mục KL.
- Vị trí của tập tin thực thi của ứng dụng trên một ổ đĩa di động.

Giá trị tiêu chí phải được quy định cho mỗi tiêu chí được sử dụng trong điều kiện. Nếu tham số của ứng dụng được khởi động khớp với giá trị của tiêu chí được quy định trong điều kiện bao gồm, quy tắc sẽ được kích hoạt. Trong trường hợp này, Kiểm soát ứng dụng khởi động sẽ thực hiện hành động được mô tả trong quy tắc. Nếu các tham số ứng dụng khớp với giá trị của tiêu chí được quy định trong điều kiện loại trừ, Kiểm soát ứng dụng khởi động sẽ không kiểm soát việc khởi động của ứng dụng.

Các quyết định được đưa ra bởi thành phần Kiểm soát ứng dụng khởi động khi một quy tắc được kích hoạt

Khi một quy tắc được kích hoạt, Kiểm soát ứng dụng khởi động sẽ cho phép người dùng (hoặc nhóm người dùng) khởi động hoặc chặn việc khởi động của ứng dụng theo quy tắc đó. Bạn có thể chọn những người dùng riêng lẻ hoặc nhóm người dùng được phép hoặc không được phép khởi động các ứng dụng kích hoạt quy tắc.

Nếu một quy tắc không quy định những người dùng được phép khởi động các ứng dụng khớp với quy tắc đó, quy tắc này được gọi là một quy tắc *chặn*.

Nếu một quy tắc không quy định bất cứ người dùng nào không được phép khởi động các ứng dụng khớp với quy tắc đó, quy tắc này được gọi là một quy tắc *cho phép*.

Một quy tắc chặn được ưu tiên hơn một quy tắc cho phép. Ví dụ, nếu một quy tắc cho phép của Kiểm soát ứng dụng khởi động đã được quy định cho một nhóm người dùng trong khi một quy tắc chặn được quy định cho một người dùng trong nhóm người dùng này, người dùng này sẽ bị chặn khỏi việc khởi động ứng dụng.

Trạng thái hoạt động của một quy tắc

Các quy tắc Kiểm soát ứng dụng khởi động có thể có một trong hai giá trị trạng thái hoạt động:

- **Bật.**

  Trạng thái hoạt động này của quy tắc có nghĩa quy tắc đang được bật.

- **Tắt.**

  Trạng thái này của quy tắc có nghĩa quy tắc đang bị tắt.

Các quy tắc Kiểm soát ứng dụng khởi động mặc định

Theo mặc định, Kiểm soát ứng dụng khởi động hoạt động trong chế độ Danh sách Đen. Thành phần này sẽ cho phép tất cả người dùng khởi động tất cả ứng dụng. Khi một người dùng cố gắng khởi động một ứng dụng bị chặn bởi quy tắc Kiểm soát ứng dụng khởi động, Kaspersky Endpoint Security sẽ chặn việc khởi động của ứng dụng này (nếu hành động **Ngăn chặn** được chọn) hoặc lưu thông tin về việc khởi động ứng dụng trong một báo cáo (nếu hành động **Thông báo** được chọn).

Quản lý các quy tắc Kiểm soát ứng dụng khởi động

Bạn có thể thực hiện hành động sau cho các quy tắc Kiểm soát ứng dụng khởi động:

- Thêm một quy tắc mới
- Tạo hoặc thay đổi điều kiện kích hoạt của một quy tắc
- Sửa trạng thái của quy tắc

  Một quy tắc Kiểm soát ứng dụng khởi động có thể được bật (hộp kiểm đối diện quy tắc được chọn) hoặc tắt (hộp kiểm đối diện quy tắc bị xóa). Ở chế độ mặc định, một quy tắc Kiểm soát ứng dụng khởi động sẽ được bật sau khi nó được tạo.
- Xóa quy tắc

Bổ sung và sửa một quy tắc Kiểm soát ứng dụng khởi động

Để bổ sung hoặc sửa một quy tắc Kiểm soát ứng dụng khởi động:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát ứng dụng khởi động**.

   Cấu hình của thành phần Kiểm soát ứng dụng khởi động sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Lựa chọn **Bật Kiểm soát ứng dụng khởi động** để có thể sửa cấu hình của thành phần này.
4. Thực hiện một trong các thao tác sau:

   - Để bổ sung một quy tắc, nhấn vào nút **Thêm**.
   - Nếu bạn muốn sửa một quy tắc hiện có, chọn nó trong danh sách các quy tắc và nhấn nút **Chỉnh sửa**.

   Cửa sổ **Quy tắc Kiểm soát ứng dụng khởi động** sẽ được mở ra.
5. Nhập hoặc sửa cấu hình của quy tắc:

   a. Trong trường **Tên quy tắc**, nhập hoặc sửa tên của quy tắc.

   b. Trong bảng **Bao gồm các điều kiện**, tạo hoặc sửa danh sách các điều kiện bao gồm kích hoạt quy tắc bằng cách nhấn các nút **Thêm**, **Chỉnh sửa**, **Gỡ bỏ** và **Chuyển đổi thành loại trừ**.

   c. Trong bảng **Loại trừ các điều kiện**, tạo hoặc sửa danh sách các điều kiện loại trừ kích hoạt quy tắc bằng cách nhấn các nút **Thêm**, **Chỉnh sửa**, **Gỡ bỏ** và **Chuyển đổi thành điều kiện bao gồm**.

   d. Nếu cần thiết, thay đổi loại điều kiện kích hoạt quy tắc:

- Để thay đổi loại điều kiện từ điều kiện bao gồm sang điều kiện loại trừ, chọn một điều kiện trong bảng **Bao gồm các điều kiện** và nhấn nút **Chuyển đổi thành loại trừ**.

- Để thay đổi loại điều kiện từ điều kiện loại trừ sang điều kiện bao gồm, chọn một điều kiện trong bảng **Loại trừ các điều kiện** và nhấn nút **Chuyển đổi thành điều kiện bao gồm**.

e. Tổng hợp hoặc sửa một danh sách người dùng và / hoặc nhóm người dùng được phép hay không được phép khởi động các ứng dụng đáp ứng được điều kiện kích hoạt quy tắc. Để thực hiện điều này, nhấn nút **Thêm** trong bảng **Quan trọng và quyền của họ**.

Cửa sổ **Chọn Người dùng hoặc Nhóm Người dùng** trong Microsoft Windows sẽ được mở ra. Cửa sổ này cho phép bạn lựa chọn người dùng và / hoặc nhóm người dùng.

Theo mặc định, giá trị **Tất cả mọi người** sẽ được thêm vào danh sách người dùng. Quy tắc này được áp dụng cho tất cả người dùng.

> Nếu không có người dùng nào được quy định trong bảng, quy tắc không thể được lưu lại.

f. Trong bảng **Quan trọng và quyền của họ**, chọn các hộp kiểm **Cho phép** hoặc **Ngăn chặn** đối diện với người dùng và / hoặc nhóm người dùng để xác định quyền khởi động ứng dụng của họ.

Hộp kiểm được chọn theo mặc định phụ thuộc vào chế độ hoạt động của Kiểm soát ứng dụng khởi động.

g. Chọn hộp kiểm **Từ chối người sử dụng khác** nếu bạn muốn tất cả người dùng không có tên trong cột **Quan trọng** và không thuộc nhóm người dùng được quy định trong cột **Quan trọng** bị chặn khỏi việc khởi động các ứng dụng khớp với điều kiện kích hoạt quy tắc.

> Nếu hộp kiểm **Từ chối người sử dụng khác** bị xóa, Kaspersky Endpoint Security sẽ không kiểm soát việc khởi động các ứng dụng của những người dùng không được quy định trong bảng **Quan trọng và quyền của họ** và không thuộc nhóm người dùng được quy định trong bảng **Quan trọng và quyền của họ**.

h. Nếu bạn muốn Kaspersky Endpoint Security coi các ứng dụng khớp với điều kiện kích hoạt quy tắc là các trình cập nhật được tin tưởng, được phép khởi động các ứng dụng khác không có quy tắc Kiểm soát ứng dụng khởi động, chọn hộp kiểm **Những cập nhật tin tưởng**.

6. Nhấn **OK**.

7. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Bổ sung một điều kiện kích hoạt cho một quy tắc Kiểm soát ứng dụng khởi động

Để bổ sung một điều kiện kích hoạt cho một quy tắc Kiểm soát ứng dụng khởi động:

1. Mở cửa sổ cấu hình ứng dụng.

2. Trong phần bên trái của cửa sổ, trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát ứng dụng khởi động**.

Cấu hình của thành phần Kiểm soát ứng dụng khởi động sẽ được hiển thị ở phần bên phải của cửa sổ.

3. Lựa chọn **Bật Kiểm soát ứng dụng khởi động** để có thể sửa cấu hình của thành phần này.

4. Thực hiện một trong các thao tác sau:

   - Nếu bạn muốn tạo một quy tắc mới và bổ sung một điều kiện kích hoạt cho nó, nhấn nút **Thêm**.
   - Nếu bạn muốn bổ sung một điều kiện kích hoạt vào một quy tắc hiện có, chọn quy tắc đó trong danh sách các quy tắc và nhấn nút **Chỉnh sửa**.

   Cửa sổ **Quy tắc Kiểm soát ứng dụng khởi động** sẽ được mở ra.

5. Trong bảng **Bao gồm các điều kiện** hoặc **Loại trừ các điều kiện**, nhấn nút **Thêm**.

Bạn có thể sử dụng danh sách thả xuống của nút **Thêm** để bổ sung nhiều điều kiện kích hoạt khác nhau vào quy tắc (xem hướng dẫn bên dưới).

Để bổ sung một điều kiện kích hoạt quy tắc dựa trên thuộc tính của các tập tin trong thư mục được chỉ định:

1. Trong danh sách thả xuống của nút **Thêm**, chọn **Điều kiện từ thuộc tính của tập tin trong thư mục quy định**.

   Cửa sổ **Lựa chọn thư mục** tiêu chuẩn của Microsoft Windows sẽ được mở ra.

2. Trong cửa sổ **Lựa chọn thư mục**, chọn một thư mục chứa các tập tin thực thi của ứng dụng có thuộc tính mà bạn muốn sử dụng làm nền tảng cho một hoặc nhiều điều kiện kích hoạt một quy tắc.

3. Nhấn **OK**.

   Cửa sổ **Thêm điều kiện** sẽ được mở ra.

4. Trong danh sách thả xuống **Hiển thị các tiêu chí**, chọn tiêu chí mà dựa vào đó bạn muốn tạo một hoặc nhiều điều kiện kích hoạt quy tắc: **Mã hash tập tin**, **Chứng nhận**, **Danh mục KL**, **Siêu dữ liệu** hoặc **Đường dẫn thư mục**.

   Kaspersky Endpoint Security không hỗ trợ mã băm tập tin MD5 và không kiểm soát việc khởi động ứng dụng dựa trên một mã băm MD5. Một mã băm SHA256 được sử dụng làm điều kiện kích hoạt quy tắc.

5. Nếu bạn chọn **Siêu dữ liệu** trong danh sách thả xuống **Hiển thị các tiêu chí**, chọn hộp kiểm đối diện các thuộc tính của tập tin thực thi mà bạn muốn sử dụng trong điều kiện kích hoạt quy tắc: **Tên tập tin**, **Phiên bản tập tin**, **Tên ứng dụng**, **Phiên bản ứng dụng**, và **Nhà cung cấp**.

   Nếu không có thuộc tính được quy định nào được chọn, quy tắc không thể được lưu lại.

6. Nếu bạn chọn **Chứng nhận** trong danh sách thả xuống **Hiển thị các tiêu chí**, chọn hộp kiểm đối diện các cấu hình mà bạn muốn sử dụng trong điều kiện kích hoạt quy tắc: **Đơn vị cấp**, **Quan trọng**, và **Vân tay**.

   Nếu không có cấu hình được quy định nào được chọn, quy tắc không thể được lưu lại.

   Không nên chỉ sử dụng các tiêu chí **Đơn vị cấp** và **Quan trọng** làm điều kiện kích hoạt quy tắc. Việc sử dụng các tiêu chí này là không ổn định.

7. Chọn hộp kiểm đối diện tên của các tập tin thực thi ứng dụng có thuộc tính mà bạn muốn bao gồm trong điều kiện kích hoạt quy tắc.

8. Nhấn nút **Tiếp theo**.

   Một danh sách các điều kiện kích hoạt quy tắc được tạo sẽ được hiển thị.

9. Trong danh sách các điều kiện kích hoạt quy tắc được tạo, chọn hộp kiểm đối diện các điều kiện kích hoạt quy tắc mà bạn muốn thêm vào quy tắc Kiểm soát ứng dụng khởi động.

10. Nhấn nút **Chấm dứt**.

Để bổ sung một điều kiện kích hoạt quy tắc dựa trên thuộc tính của các ứng dụng được khởi động trên máy tính:

1. Trong danh sách thả xuống của nút **Thêm**, chọn **Điều kiện từ thuộc tính của ứng dụng khởi động**.

2. Trong cửa sổ **Thêm điều kiện**, trong danh sách thả xuống **Hiển thị các tiêu chí**, chọn tiêu chí mà dựa vào đó bạn muốn tạo một hoặc nhiều điều kiện kích hoạt quy tắc: **Mã băm tập tin**, **Chứng nhận**, **Hạng mục KL**, **Siêu dữ liệu** hoặc **Đường dẫn thư mục**.

3. Nếu bạn chọn **Siêu dữ liệu** trong danh sách thả xuống **Hiển thị các tiêu chí**, chọn hộp kiểm đối diện các thuộc tính của tập tin thực thi mà bạn muốn sử dụng trong điều kiện kích hoạt quy tắc: **Tên tập tin**, **Phiên bản tập tin**, **Tên ứng dụng**, **Phiên bản ứng dụng**, và **Nhà cung cấp**.

   Nếu không có thuộc tính được quy định nào được chọn, quy tắc không thể được lưu lại.

4. Nếu bạn chọn **Chứng nhận** trong danh sách thả xuống **Hiển thị các tiêu chí**, chọn hộp kiểm đối diện các cấu hình mà bạn muốn sử dụng trong điều kiện kích hoạt quy tắc: **Đơn vị cấp**, **Quan trọng**, và **Vân tay**.

   Nếu không có cấu hình được quy định nào được chọn, quy tắc không thể được lưu lại.

   > Không nên chỉ sử dụng các tiêu chí **Đơn vị cấp** và **Quan trọng** làm điều kiện kích hoạt quy tắc. Việc sử dụng các tiêu chí này là không ổn định.

5. Chọn hộp kiểm đối diện tên của các tập tin thực thi ứng dụng có thuộc tính mà bạn muốn bao gồm trong điều kiện kích hoạt quy tắc.

6. Nhấn nút **Tiếp theo**.

   Một danh sách các điều kiện kích hoạt quy tắc được tạo sẽ được hiển thị.

7. Trong danh sách các điều kiện kích hoạt quy tắc được tạo, chọn hộp kiểm đối diện các điều kiện kích hoạt quy tắc mà bạn muốn thêm vào quy tắc Kiểm soát ứng dụng khởi động.

8. Nhấn nút **Chấm dứt**.

Để bổ sung một điều kiện kích hoạt quy tắc dựa trên một hạng mục KL:

1. Trong danh sách thả xuống bên dưới nút **Thêm**, chọn **Điều kiện "Danh mục KL"**.

   Một *hạng mục KL* là một danh sách các ứng dụng có thuộc tính chủ đề giống nhau. Danh sách này được duy trì bởi các chuyên gia Kaspersky. Ví dụ, hạng mục KL của "Các ứng dụng Office" bao gồm các ứng dụng từ bộ phần mềm Microsoft Office, Adobe® Acrobat®, v.v...

2. Trong cửa sổ **Điều kiện "Danh mục KL"**, chọn hộp kiểm đối diện tên của các danh mục KL mà dựa vào đó bạn muốn tạo các điều kiện kích hoạt quy tắc.

3. Nhấn **OK**.

Để bổ sung một điều kiện kích hoạt quy tắc tùy chỉnh:

1. Trong danh sách thả xuống của nút **Thêm**, chọn **Tùy chỉnh điều kiện**.
2. Trong cửa sổ **Tùy chỉnh điều kiện**, nhấn nút **Lựa chọn** và quy định đường dẫn đến tập tin thực thi của ứng dụng.
3. Chọn tiêu chí mà dựa vào đó bạn muốn tạo một điều kiện kích hoạt quy tắc: **Mã băm tập tin**, **Chứng nhận**, **Siêu dữ liệu** hoặc **Đường dẫn đến tập tin hoặc thư mục**.

   Nếu bạn đang sử dụng một liên kết tượng trưng trong trường **Đường dẫn đến tập tin hoặc thư mục**, bạn nên diễn giải liên kết tượng trưng đó để quy tắc Kiểm soát ứng dụng khởi động có thể hoạt động tốt. Để làm điều này, nhấn vào nút **Diễn giải liên kết tượng trưng**.

4. Nếu cần thiết, hãy thiết lập cấu hình của tiêu chí được chọn.
5. Nhấn **OK**.

Để bổ sung một điều kiện kích hoạt quy tắc dựa trên thông tin về ổ đĩa có chứa tập tin thực thi của một ứng dụng:

1. Trong danh sách thả xuống của nút **Thêm**, chọn **Điều kiện bởi tập tin điều khiển**.
2. Trong cửa sổ **Điều kiện bởi tập tin điều khiển**, trong danh sách thả xuống **Trình điều khiển**, chọn kiểu ổ đĩa mà việc các ứng dụng được khởi động từ đó sẽ được coi là một điều kiện kích hoạt quy tắc.
3. Nhấn **OK**.

Thay đổi trạng thái của một quy tắc Kiểm soát ứng dụng khởi động

Để thay đổi trạng thái của một quy tắc Kiểm soát ứng dụng khởi động:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát ứng dụng khởi động**.

   Cấu hình của thành phần Kiểm soát ứng dụng khởi động sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Lựa chọn **Bật Kiểm soát ứng dụng khởi động** để có thể sửa cấu hình của thành phần này.
4. Chọn quy tắc có trạng thái mà bạn muốn sửa.
5. Trong cột **Trạng thái**, thực hiện các thao tác sau:
   - Nếu bạn muốn bật một quy tắc, chọn hộp kiểm đối diện với quy tắc đó.
   - Nếu bạn muốn tắt một quy tắc, xóa hộp kiểm đối diện với quy tắc đó.
6. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Kiểm tra quy tắc Kiểm soát ứng dụng khởi động

Để đảm bảo các quy tắc Kiểm soát Khởi động Ứng dụng không chặn ứng dụng cần cho công việc, bạn nên đặt các quy tắc mới được tạo vào chế độ kiểm tra để phân tích hoạt động của chúng.

Một phân tích về hoạt động của các quy tắc Kiểm soát Khởi động Ứng dụng yêu cầu bạn xem lại các sự kiện Kiểm soát Khởi động Ứng dụng được báo cáo đến Kaspersky Security Center. Nếu tất cả các ứng dụng cần cho công việc của người sử dụng máy tính đều được phép khởi động, các quy tắc này đã được tạo đúng cách. Nếu không, bạn nên sửa lại các cấu hình của quy tắc mà bạn đã tạo.

Chế độ kiểm tra cho các quy tắc Kiểm soát Khởi động Ứng dụng bị tắt theo mặc định.

Để kiểm tra các quy tắc Kiểm soát Khởi động Ứng dụng:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát ứng dụng khởi động**.

   Cấu hình của thành phần Kiểm soát ứng dụng khởi động sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Lựa chọn **Bật Kiểm soát ứng dụng khởi động** để có thể sửa cấu hình của thành phần này.
4. Trong danh sách thả xuống **Chế độ Kiểm soát ứng dụng khởi động**, chọn một trong các mục sau:
   - **Danh sách Đen**, nếu bạn muốn cho phép khởi động tất cả các ứng dụng, ngoại trừ các ứng dụng được quy định trong quy tắc chặn.
   - **Danh sách Trắng**, nếu bạn muốn chặn khởi động tất cả các ứng dụng, ngoại trừ các ứng dụng được quy định trong quy tắc cho phép.
5. Trong danh sách thả xuống **Hành động**, chọn **Thông báo**.
6. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Kaspersky Endpoint Security sẽ không chặn các ứng dụng mà việc khởi động của chúng bị cấm bởi các quy tắc Kiểm soát Khởi động Ứng dụng, nhưng sẽ thông báo về sự kiện này đến Máy chủ Quản trị.

Sửa mẫu thông điệp Kiểm soát ứng dụng khởi động

Khi một người dùng cố gắng khởi động một ứng dụng bị chặn bởi quy tắc Kiểm soát ứng dụng khởi động, Kaspersky Endpoint Security sẽ hiển thị một thông điệp cho biết ứng dụng đã bị chặn khởi động. Nếu người dùng tin rằng ứng dụng đã bị chặn nhầm, người dùng có thể sử dụng liên kết trong nội dung thông điệp để gửi một thông điệp đến quản trị viên mạng doanh nghiệp cục bộ.

Các mẫu đặc biệt có thể được sử dụng cho thông điệp được hiển thị khi một ứng dụng bị chặn khởi động cũng như cho thông điệp được gửi đến quản trị viên. Bạn có thể sửa mẫu thông điệp.

Để sửa một mẫu thông điệp:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát ứng dụng khởi động**.

   Cấu hình của thành phần Kiểm soát ứng dụng khởi động sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Lựa chọn **Bật Kiểm soát ứng dụng khởi động** để có thể sửa cấu hình của thành phần này.

4. Nhấn nút **Mẫu**.

   Cửa sổ **Tin nhắn mẫu** sẽ được mở ra.

5. Thực hiện một trong các thao tác sau:

   - Nếu bạn muốn sửa mẫu thông điệp được hiển thị khi một ứng dụng bị chặn khởi động, chọn thẻ **Thông báo**.

   - Nếu bạn muốn sửa mẫu thông điệp được gửi đến quản trị viên mạng LAN, chọn thẻ **Thông điệp đến quản trị viên**.

6. Sửa mẫu của thông điệp được hiển thị khi một ứng dụng bị chặn khởi động hoặc mẫu thông điệp được gửi đến quản trị viên. Để làm điều này, sử dụng các nút **Mặc định** và **Biến số**.

7. Nhấn **OK**.

8. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Thông tin về chế độ hoạt động của Kiểm soát ứng dụng khởi động

Thành phần Kiểm soát ứng dụng khởi động hoạt động trong hai chế độ:

- **Danh sách Đen**. Trong chế độ này, Kiểm soát ứng dụng khởi động sẽ cho phép tất cả người dùng được bắt đầu tất cả các ứng dụng, ngoại trừ các ứng dụng được quy định trong quy tắc chặn của Kiểm soát ứng dụng khởi động.

  Chế độ Kiểm soát ứng dụng khởi động này được bật theo mặc định.

- **Danh sách Trắng**. Trong chế độ này, Kiểm soát ứng dụng khởi động sẽ chặn tất cả người dùng khỏi việc bắt đầu bất kỳ ứng dụng nào, ngoại trừ các ứng dụng được quy định trong quy tắc cho phép của Kiểm soát ứng dụng khởi động.

  Nếu quy tắc cho phép của Kiểm soát ứng dụng khởi động được thiết lập đầy đủ, thành phần này sẽ chặn việc khởi động tất cả các ứng dụng mới chưa được xác nhận bởi quản trị viên mạng LAN, và cho phép hoạt động của hệ điều hành cũng như của các ứng dụng được tin tưởng mà người dùng sử dụng trong công việc của họ.

Mỗi chế độ có hai hành động có thể được thực hiện trên các ứng dụng đang chạy: Kaspersky Endpoint Security có thể chặn việc khởi động các ứng dụng hoặc thông báo với người dùng về việc khởi động của một ứng dụng khớp với các điều kiện của quy tắc Kiểm soát ứng dụng khởi động.

Kiểm soát ứng dụng khởi động có thể được thiéte lập để hoạt động trong cả hai chế độ này bằng cách sử dụng giao diện cục bộ của Kaspersky Endpoint Security, và bằng Kaspersky Security Center.

Tuy nhiên, Kaspersky Security Center cung cấp các công cụ không sẵn có trong giao diện cục bộ của Kaspersky Endpoint Security, ví dụ như các công cụ cần cho những tác vụ sau đây:

- Tạo hạng mục ứng dụng.

  Các quy tắc Kiểm soát ứng dụng khởi động được tạo trong Bảng điều khiển Quản trị Kaspersky Security Center sẽ được dựa trên những hạng mục ứng dụng tùy chỉnh, và không chỉ trên các điều kiện bao gồm và loại trừ như trong giao diện cục bộ của Kaspersky Endpoint Security.

- Thu thập thông tin về các ứng dụng được cài đặt trên máy tính LAN.

Đây là lý do bạn nên sử dụng Kaspersky Security Center để thiết lập hoạt động của thành phần Kiểm soát ứng dụng khởi động.

Chọn chế độ Kiểm soát ứng dụng khởi động

Để chọn chế độ Kiểm soát ứng dụng khởi động:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát ứng dụng khởi động**.

   Cấu hình của thành phần Kiểm soát ứng dụng khởi động sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Lựa chọn **Bật Kiểm soát ứng dụng khởi động** để có thể sửa cấu hình của thành phần này.
4. Trong danh sách thả xuống **Chế độ Kiểm soát ứng dụng khởi động**, chọn một trong các mục sau:

   - **Danh sách Đen**, nếu bạn muốn cho phép khởi động tất cả các ứng dụng, ngoại trừ các ứng dụng được quy định trong quy tắc chặn.
   - **Danh sách Trắng**, nếu bạn muốn chặn khởi động tất cả các ứng dụng, ngoại trừ các ứng dụng được quy định trong quy tắc cho phép.

     Khi chế độ này được lựa chọn, hai quy tắc Kiểm soát ứng dụng khởi động sẽ được tạo theo mặc định: **Hình ảnh Vàng** và **Những cập nhật tin tưởng**. Bạn không thể xóa các quy tắc này. Cấu hình của các quy tắc này không thể được sửa đổi. Bạn có thể bật hoặc tắt các quy tắc này bằng cách lựa chọn và xóa hộp kiểm đối diện với quy tắc tương ứng. Theo mặc định, quy tắc **Hình ảnh Vàng** sẽ được bật, và quy tắc **Trình Cập nhật được Tin tưởng** bị tắt. Tất cả người dùng đều được phép khởi động các ứng dụng khớp với điều kiện kích hoạt của những quy tắc này.

   Tất cả các quy tắc được tạo trong chế độ được chọn đều được lưu lại sau khi chế độ được thay đổi, để quy tắc có thể được sử dụng lại. Để quay lại sử dụng các quy tắc này, tất cả những gì bạn cần làm là chọn chế độ cần thiết trong danh sách thả xuống **Chế độ Kiểm soát ứng dụng khởi động**.
5. Trong danh sách thả xuống **Hành động**, chọn hành động được thực hiện bởi thành phần khi người dùng cố gắng khởi động một ứng dụng bị chặn bởi các quy tắc Kiểm soát ứng dụng khởi động.
6. Chọn hộp kiểm **Giám sát DLL và trình điều khiển** nếu bạn muốn Kaspersky Endpoint Security giám sát việc nạp các mô-đun DLL khi ứng dụng được khởi động bởi người dùng.

   Thông tin về mô-đun và ứng dụng nạp mô-đun sẽ được lưu vào một báo cáo.

   Nếu hộp kiểm được chọn, các mô-đun DLL và trình điều khiển sẽ được giám sát từ trước khi Kaspersky Endpoint Security được bắt đầu. Để cấu hình việc giám sát sau đó của tất cả các mô-đun DLL và trình điều khiển trước khi khởi động ứng dụng, khởi động lại máy tính sau khi lựa chọn hộp kiểm **Giám sát DLL và trình điều khiển**. Nếu bạn không thể khởi động lại máy tính, sau khi lựa chọn hộp kiểm **Giám sát DLL và trình điều khiển**, bạn có thể nạp các mô-đun DLL và trình điều khiển trong khi Kaspersky Endpoint Security đang chạy. Trong trường hợp này, việc giám sát sẽ chỉ có hiệu lực cho các mô-đun DLL và trình điều khiển được nạp trong khi Kaspersky Endpoint Security đang chạy.

Khi giám sát các mô-đun DLL và trình điều khiển, bạn không nên sử dụng các quy tắc Kiểm soát ứng dụng khởi động được tạo dựa trên các danh mục KL. Việc xác định danh mục KL (bao gồm trong quy tắc "Hệ điều hành và các thành phần hệ điều hành") cho các mô-đun DLL và trình điều khiển có thể không hoạt động đúng cách. Cụ thể, quy tắc “Hệ điều hành và các thành phần hệ điều hành” đã được tạo theo mặc định và không được phân phối khi khởi chạy mô-đun DLL và trình điều khiển. Khi bật chức năng này, bạn cần tạo các quy tắc cho phép riêng biệt cho các mô-đun DLL và trình điều khiển. Việc sử dụng chức năng **Kiểm soát DLL và trình điều khiển** nếu các quy tắc cho phép đó không tồn tại có thể khiến hệ thống bị bất ổn định.

Chúng tôi khuyến nghị bật chức năng mật khẩu bảo vệ cho việc cấu hình thiết lập chương trình, để bạn có thể tắt các quy tắc cho phép chặn việc khởi chạy của những mô-đun DLL và trình điều khiển thiết yếu nhưng đồng thời vẫn không thay đổi thiết lập chính sách của Kaspersky Security Center.

7. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Quản lý các quy tắc Kiểm soát ứng dụng khởi động sử dụng Kaspersky Security Center

Phần này chứa thông tin về việc sử dụng Kaspersky Security Center để thiết lập các quy tắc Kiểm soát ứng dụng khởi động, và cung cấp các khuyến nghị về việc sử dụng Kiểm soát ứng dụng khởi động một cách tối ưu.

Thu thập thông tin về các ứng dụng được cài đặt trên máy tính của người dùng

Để tạo ra các quy tắc Kiểm soát ứng dụng khởi động tối ưu, trước hết bạn nên tìm hiểu về các ứng dụng được sử dụng trên các máy tính trên mạng máy tính cục bộ. Để làm điều này, bạn có thể nhận các thông tin như sau:

- Nhà cung cấp, phiên bản, ngôn ngữ địa phương của các ứng dụng được sử dụng trên mạng LAN doanh nghiệp.
- Tần suất cập nhật ứng dụng.
- Các chính sách sử dụng ứng dụng được áp dụng bởi công ty (đây có thể là các chính sách bảo mật hoặc chính sách quản trị).
- Vị trí lưu trữ của các gói phân phối ứng dụng.

Thông tin về các ứng dụng được sử dụng trên mạng LAN doanh nghiệp được cung cấp trong các thư mục **Registry ứng dụng** và **Tập tin thực thi**. Các thư mục **Registry ứng dụng** và **Tập tin thực thi** được đặt trong thư mục **Quản lý ứng dụng** trên cây Bảng điều khiển Quản trị của Kaspersky Security Center.

Thư mục **Registry ứng dụng** chứa danh sách các ứng dụng được phát hiện bởi Network Agent cài đặt trên máy khách.

Thư mục **Tập tin thực thi** chứa một danh sách gồm tất cả các tập tin thực đã từng được khởi động trên các máy khách hoặc đã được phát hiện trong tác vụ lưu kho của Kaspersky Endpoint Security.

Để xem thông tin chung về một ứng dụng và các tập tin thực thi của nó, cùng danh sách các máy tính có cài đặt ứng dụng đó, mở cửa sổ thuộc tính của một ứng dụng được chọn trong thư mục **Registry ứng dụng** hoặc thư mục **Tập tin thực thi**.

Tạo hạng mục ứng dụng

Để có thể tạo các quy tắc một cách tiện lợi hơn, bạn có thể tạo các hạng mục ứng dụng và sử dụng chúng khi tạo các quy tắc Kiểm soát ứng dụng khởi động.

Bạn nên tạo một hạng mục "Ứng dụng làm việc" bao gồm các nhóm ứng dụng tiêu chuẩn được sử dụng tại công ty. Nếu các nhóm người dùng khác nhau sử dụng các nhóm ứng dụng khác nhau trong công việc của họ, một hạng mục ứng dụng riêng cũng có thể được tạo cho mỗi nhóm người dùng.

Để tạo một hạng mục ứng dụng:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Trong cây Bảng điều khiển Quản trị, chọn thư mục **Bổ sung** → **Quản lý ứng dụng** → **Hạng mục ứng dụng**.
3. Nhấn nút **Tạo hạng mục** trong không gian làm việc.
   Trình hướng dẫn tạo hạng mục người dùng sẽ được bắt đầu.
4. Làm theo chỉ dẫn của trình hướng dẫn tạo hạng mục người dùng.

Tạo các quy tắc Kiểm soát ứng dụng khởi động sử dụng Kaspersky Security Center

Để tạo một quy tắc Kiểm soát ứng dụng khởi động sử dụng Kaspersky Security Center:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, mở thư mục với tên của nhóm quản trị chứa máy khách liên quan.
3. Trong không gian làm việc, chọn thẻ **Chính sách**.
4. Chọn chính sách cần thiết.
5. Mở cửa sổ **Thuộc tính: <Tên chính sách>** sử dụng một trong những phương pháp sau đây:
   - Trong menu ngữ cảnh của chính sách, chọn **Thuộc tính**.
   - Nhấn vào liên kết **Thiết lập chính sách** được đặt ở phần bên phải của không gian làm việc của Bảng điều khiển Quản trị.
6. Trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát ứng dụng khởi động**.
   Cấu hình của thành phần Kiểm soát ứng dụng khởi động sẽ được hiển thị ở phần bên phải của cửa sổ.

7. Nhấn vào nút **Thêm**.

   Cửa sổ **Quy tắc Kiểm soát ứng dụng khởi động** sẽ được mở ra.

8. Trong danh sách thả xuống **Danh mục**, chọn hạng mục ứng dụng được tạo mà dựa vào đó bạn muốn tạo một quy tắc.

9. Quy định danh sách người dùng và / hoặc nhóm người dùng mà bạn muốn thiết lập quyền khởi động ứng dụng từ hạng mục được chọn. Để làm điều này, trong bảng **Quan trọng và quyền của họ**, nhấn nút **Thêm**.

   Cửa sổ **Chọn Người dùng hoặc Nhóm Người dùng** tiêu chuẩn trong Microsoft Windows sẽ được mở ra. Cửa sổ này cho phép bạn lựa chọn người dùng và / hoặc nhóm người dùng.

10. Trong bảng **Quan trọng và quyền của họ**:

    - Nếu bạn muốn cho phép người dùng và / hoặc nhóm người dùng khởi động các ứng dụng thuộc hạng mục được chọn, chọn hộp kiểm **Cho phép** đối diện những người dùng đó.

    - Nếu bạn muốn chặn người dùng và / hoặc nhóm người dùng khỏi việc khởi động các ứng dụng thuộc hạng mục được chọn, chọn hộp kiểm **Ngăn chặn** đối diện những người dùng đó.

11. Chọn hộp kiểm **Từ chối người sử dụng khác** nếu bạn muốn tất cả người dùng không có tên trong cột **Quan trọng** và không thuộc nhóm người dùng được quy định trong cột **Quan trọng** bị chặn khỏi việc khởi động các ứng dụng thuộc hạng mục được chọn.

12. Nếu bạn muốn Kaspersky Endpoint Security coi các ứng dụng thuộc hạng mục được quy định trong quy tắc là các trình cập nhật được tin tưởng, được phép khởi động các ứng dụng khác không có quy tắc Kiểm soát ứng dụng khởi động, chọn hộp kiểm **Những cập nhật tin tưởng**.

13. Nhấn **OK**.

14. Trong mục **Kiểm soát ứng dụng khởi động** của cửa sổ thuộc tính chính sách, nhấn nút **Áp dụng**.

Thay đổi trạng thái của một quy tắc Kiểm soát ứng dụng khởi động sử dụng Kaspersky Security Center

Để thay đổi trạng thái của một quy tắc Kiểm soát ứng dụng khởi động:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.

2. Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, mở thư mục với tên của nhóm quản trị chứa máy khách liên quan.

3. Trong không gian làm việc, chọn thẻ **Chính sách**.

4. Chọn chính sách cần thiết.

5. Mở cửa sổ **Thuộc tính: <Tên chính sách>** sử dụng một trong những phương pháp sau đây:

   - Trong menu ngữ cảnh của chính sách, chọn **Thuộc tính**.

   - Nhấn vào liên kết **Thiết lập chính sách** được đặt ở phần bên phải của không gian làm việc của Bảng điều khiển Quản trị.

6. Trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát ứng dụng khởi động**.
   Cấu hình của thành phần Kiểm soát ứng dụng khởi động sẽ được hiển thị ở phần bên phải của cửa sổ.
7. Chọn quy tắc Kiểm soát ứng dụng khởi động mà bạn muốn thay đổi trạng thái.
8. Trong cột **Trạng thái**, thực hiện một trong các thao tác sau:
   - Nếu bạn muốn bật một quy tắc, chọn hộp kiểm đối diện với quy tắc đó.
   - Nếu bạn muốn tắt một quy tắc, xóa hộp kiểm đối diện với quy tắc đó.
9. Nhấn nút **Áp dụng**.

Kiểm soát Đặc quyền Ứng dụng

Thành phần này có thể được sử dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Microsoft Windows cho máy trạm. Thành phần này không thể được sử dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Microsoft Windows cho máy chủ tập tin.

Mục này chứa thông tin về Kiểm soát Đặc quyền Ứng dụng và chỉ dẫn cách để thiết lập cấu hình thành phần.

Thông tin về Kiểm soát Đặc quyền Ứng dụng

Kiểm soát Đặc quyền Ứng dụng ngăn chặn các ứng dụng khỏi việc thực hiện các hành động có thể gây nguy hiểm cho hệ điều hành và đảm bảo kiểm soát quyền truy cập vào các tài nguyên hệ điều hành cũng như dữ liệu danh tính.

Thành phần này kiểm soát hoạt động của các ứng dụng, bao gồm quyền truy cập của chúng đến tài nguyên được bảo vệ (ví dụ như các tập tin và thư mục, khóa registry) bằng *các quy tắc kiểm soát ứng dụng*. Quy tắc quản lý ứng dụng là một nhóm các hạn chế được áp dụng cho nhiều hành động khác nhau của ứng dụng trong hệ điều hành và cho các quyền truy cập tài nguyên máy tính.

Hoạt động mạng của các ứng dụng sẽ bị giám sát bởi thành phần Tường lửa.

Khi một ứng dụng được khởi động lần đầu tiên, Kiểm soát Đặc quyền Ứng dụng sẽ quét ứng dụng đó và đặt nó vào một nhóm tin tưởng. Một nhóm tin tưởng quy định các quy tắc kiểm soát ứng dụng được Kaspersky Endpoint Security áp dụng khi kiểm soát hoạt động của các ứng dụng trong nhóm đó.

Chúng tôi khuyến nghị bạn tham gia Kaspersky Security Network để Kiểm soát Đặc quyền Ứng dụng có thể hoạt động hiệu quả hơn. Dữ liệu được nhận thông qua Kaspersky Security Network sẽ cho phép bạn xếp các ứng dụng vào các nhóm một cách chính xác hơn nữa và áp dụng các quy tắc kiểm soát ứng dụng tối ưu.

Lần tiếp theo ứng dụng được khởi chạy, Kiểm soát Đặc quyền Ứng dụng sẽ xác minh tính toàn vẹn của ứng dụng. Nếu ứng dụng không thay đổi, thành phần sẽ áp dụng các quy tắc kiểm soát ứng dụng hiện tại cho nó. Nếu ứng dụng đã được thay đổi, Kiểm soát Đặc quyền Ứng dụng sẽ quét lại nó như khi nó được khởi động lần đầu tiên.

Giới hạn kiểm soát đối với các thiết bị âm thanh và video

Thông tin về bảo vệ dòng truyền phát âm thanh

Bảo vệ dòng truyền phát âm thanh có những lưu ý đặc biệt sau:

- Thành phần Kiểm soát Đặc quyền Ứng dụng phải được bật để chức năng này có thể hoạt động.

- Nếu ứng dụng bắt đầu nhận dòng âm thanh trước khi thành phần Kiểm soát Đặc quyền Ứng dụng được bắt đầu, Kaspersky Endpoint Security sẽ cho phép ứng dụng nhận dòng âm thanh đó và không hiển thị bất kỳ thông báo nào.
- Nếu bạn đã di chuyển ứng dụng vào nhóm **Không Tin tưởng** hoặc **Hạn chế cao** sau khi ứng dụng bắt đầu nhận dòng âm thanh, Kaspersky Endpoint Security sẽ cho phép ứng dụng nhận dòng âm thanh đó và không hiển thị bất kỳ thông báo nào.
- Sau khi cấu hình quyền truy cập của ứng dụng đến các thiết bị ghi âm đã được thay đổi (ví dụ như ứng dụng đã bị cấm nhận dòng âm thanh trong cửa sổ thiết lập Quản lý Ứng dụng), ứng dụng này phải được khởi động lại để nó không thể tiếp tục nhận dòng âm thanh.
- Việc kiểm soát truy cập đến dòng truyền phát âm thanh từ thiết bị ghi âm không tùy thuộc vào cấu hình truy cập webcam của ứng dụng.
- Kaspersky Endpoint Security chỉ bảo vệ quyền truy cập đến các microphone tích hợp và lắp ngoài. Các thiết bị truyền phát âm thanh khác không được hỗ trợ.
- Kaspersky Endpoint Security không đảm bảo tính năng bảo vệ dòng âm thanh từ các thiết bị như máy ảnh DSLR, máy quay lưu động, và máy quay hành động.

Các cân nhắc đặc biệt đối với hoạt động của các thiết bị âm thanh và video trong quá trình cài đặt và nâng cấp Kaspersky Endpoint Security

Khi bạn chạy ứng dụng ghi lại hoặc phát lại âm thanh hay vidieo lần đầu tiên kể từ khi cài đặt Kaspersky Endpoint Security, chức năng ghi lại hoặc phát lại âm thanh hay video có thể bị ngắt quãng. Điều này là cần thiết để bật chức năng kiểm soát quyền truy cập đến các thiết bị ghi âm của các ứng dụng. Dịch vụ hệ thống kiểm soát phần cứng âm thanh sẽ được khởi động lại khi Kaspersky Endpoint Security được chạy lần đầu tiên.

Thông tin về quyền truy cập đến webcam của các ứng dụng

Chức năng bảo vệ truy cập webcam có các cân nhắc và hạn chế đặc biệt sau đây:

- Ứng dụng sẽ kiểm soát các video và hình ảnh tĩnh có được từ quá trình xử lý dữ liệu webcam.
- Ứng dụng kiểm soát dòng âm thanh nếu nó là một phần của dòng truyền phát video được nhận từ webcam.
- Ứng dụng sẽ chỉ kiểm soát các webcam được kết nối qua cổng USB hoặc IEEE1394 được hiển thị trong dưới dạng **Thiết bị Hình ảnh** trong Windows Device Manager.

Webcam được hỗ trợ

Kaspersky Endpoint Security hỗ trợ các webcam sau:

- Logitech HD Webcam C270
- Logitech HD Webcam C310
- Logitech Webcam C210
- Logitech Webcam Pro 9000

- Logitech HD Webcam C525
- Microsoft LifeCam VX-1000
- Microsoft LifeCam VX-2000
- Microsoft LifeCam VX-3000
- Microsoft LifeCam VX-800
- Microsoft LifeCam Cinema

Kaspersky không đảm bảo việc hỗ trợ cho các webcam không được quy định trong danh sách này.

Bật và tắt Kiểm soát Đặc quyền Ứng dụng

Theo mặc định, Kiểm soát Đặc quyền Ứng dụng sẽ được bật và chạy trong một chế độ được khuyến nghị bởi các chuyên gia của Kaspersky. Bạn có thể tắt Kiểm soát Đặc quyền Ứng dụng nếu cần thiết.

Có hai cách để bật hoặc tắt thành phần này:

- Trên thẻ **Bảo vệ và Kiểm soát** của cửa sổ chính của ứng dụng
- Từ cửa sổ cấu hình ứng dụng.

Để bật hoặc tắt Kiểm soát Đặc quyền Ứng dụng trên thẻ Bảo vệ và Kiểm soát của cửa sổ chính của ứng dụng:

1. Mở cửa sổ chính của ứng dụng.
2. Chọn thẻ **Bảo vệ và Kiểm soát**.
3. Nhấn vào mục **Bảng kiểm soát**.
   Mục **Bảng kiểm soát** sẽ được mở ra.
4. Nhấn phải chuột để hiển thị menu ngữ cảnh của dòng có chứa thông tin về thành phần Kiểm soát Đặc quyền Ứng dụng.
   Một menu để chọn hành động đối với thành phần sẽ được mở ra.
5. Thực hiện một trong các thao tác sau:
   - Để bật Kiểm soát Đặc quyền Ứng dụng, chọn **Bắt đầu**.
     Biểu tượng trạng thái của thành phần , được hiển thị ở bên trái của dòng Kiểm soát Đặc quyền Ứng dụng sẽ được chuyển sang biểu tượng .
   - Để tắt thành phần Kiểm soát Đặc quyền Ứng dụng, chọn **Dừng**.
     Biểu tượng trạng thái của thành phần , được hiển thị ở bên trái của dòng Kiểm soát Đặc quyền Ứng dụng sẽ được chuyển sang biểu tượng .

Để bật hoặc tắt Kiểm soát Đặc quyền Ứng dụng từ cửa sổ cấu hình ứng dụng:

1. Mở cửa sổ cấu hình ứng dụng.

2. Trong phần bên trái của cửa sổ, trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát Đặc quyền Ứng dụng**.

   Cấu hình của thành phần Kiểm soát Đặc quyền Ứng dụng sẽ được hiển thị ở phần bên phải của cửa sổ.

3. Trong phần bên phải của cửa sổ, thực hiện một trong các thao tác sau:

   - Để bật Kiểm soát Đặc quyền Ứng dụng, chọn hộp kiểm **Bật Kiểm soát Đặc quyền Ứng dụng**.
   - Để tắt Kiểm soát Đặc quyền Ứng dụng, xóa hộp kiểm **Bật Kiểm soát Đặc quyền Ứng dụng**.

4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Quản lý các nhóm tin tưởng ứng dụng

Khi mỗi ứng dụng được khởi động lần đầu tiên, thành phần Kiểm soát Đặc quyền Ứng dụng sẽ kiểm tra tính bảo mật của ứng dụng đó và đặt nó vào một nhóm tin tưởng.

Ở giai đoạn đầu tiên của tác vụ quét ứng dụng, Kaspersky Endpoint Security sẽ tìm kiếm trong cơ sở dữ liệu nội bộ của các ứng dụng đã biết để đối chiếu các đề mục và đồng thời gửi một yêu cầu đến cơ sở dữ liệu Kaspersky Security Network (nếu có kết nối Internet khả dụng). Dựa trên kết quả tìm kiếm trong cơ sở dữ liệu nội bộ và trên cơ sở dữ liệu của Kaspersky Security Network, ứng dụng đó sẽ được đặt vào một nhóm tin tưởng. Mỗi khi ứng dụng được khởi động, Kaspersky Endpoint Security sẽ gửi một truy vấn mới đến cơ sở dữ liệu KSN và đặt ứng dụng vào một nhóm tin tưởng khác nếu danh tiếng của nhóm tin tưởng này trong cơ sở dữ liệu KSN đã thay đổi.

Bạn có thể chọn một nhóm tin tưởng để Kaspersky Endpoint Security tự động gán tất cả các ứng dụng không xác định vào đó. Các ứng dụng đã được khởi động trước Kaspersky Endpoint Security sẽ tự động được di chuyển vào nhóm tin tưởng được quy định trong cửa sổ **Lựa chọn nhóm tin tưởng**.

Thành phần này chỉ kiểm soát hoạt động mạng của các ứng dụng đã được khởi động trước Kaspersky Endpoint Security dựa trên quy tắc mạng được thiết lập trong cấu hình Tường lửa.

Thiết lập cấu hình để gán ứng dụng vào các nhóm tin tưởng

Nếu việc tham gia Kaspersky Security Network được bật, Kaspersky Endpoint Security sẽ gửi đến KSN một truy vấn đề danh tiếng của một ứng dụng mỗi khi ứng dụng được khởi động. Dựa trên phản hồi từ KSN, ứng dụng có thể sẽ được di chuyển đến một nhóm tin tưởng khác với nhóm được quy định trong cấu hình Kiểm soát Đặc quyền Ứng dụng.

Để thiết lập cấu hình để đặt ứng dụng vào các nhóm tin tưởng:

1. Mở cửa sổ cấu hình ứng dụng.

2. Trong phần bên trái của cửa sổ, trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát Đặc quyền Ứng dụng**.

   Cấu hình của thành phần Kiểm soát Đặc quyền Ứng dụng sẽ được hiển thị ở phần bên phải của cửa sổ.

3. Nếu bạn muốn tự động đặt các ứng dụng có chữ ký điện tử từ các nhà cung cấp được tin tưởng vào nhóm Được Tin tưởng, chọn hộp kiểm **Những chương trình tin tưởng mà có chữ ký điện tử**.

   Nhà cung cấp được tin tưởng là những nhà cung cấp phần mềm được Kaspersky thêm vào nhóm tin tưởng. Bạn cũng có thể thêm chứng chỉ nhà cung cấp vào kho chứng chỉ hệ thống được tin tưởng theo cách thủ công.

4. Chọn cách gán ứng dụng không xác định vào các nhóm tin tưởng:

   - Để sử dụng phân tích suy nghiệm cho việc phân bổ các ứng dụng không xác định vào các nhóm tin tưởng, chọn **Sử dụng phân tích theo hành vi để định nghĩa các nhóm** và quy định khoảng thời gian sẽ được phân bổ cho việc bắt đầu các ứng dụng trong trường **Thời gian tối đa để xác định nhóm**.

   - Nếu bạn muốn gán tất cả các ứng dụng không xác định vào một nhóm tin tưởng cụ thể, chọn **Tự động di chuyển đến nhóm** và chọn nhóm tin tưởng phù hợp trong danh sách thả xuống.

     Vì mục đích bảo mật, nhóm **Tin tưởng** sẽ không được bao gồm trong các giá trị của cấu hình **Tự động di chuyển đến nhóm**.

5. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Sửa đổi một nhóm tin tưởng

Khi một ứng dụng được khởi động lần đầu tiên, Kaspersky Endpoint Security sẽ tự động đặt ứng dụng đó vào một nhóm tin tưởng. Bạn có thể di chuyển ứng dụng sang một nhóm tin tưởng khác một cách thủ công nếu cần thiết.

Các chuyên gia Kaspersky không khuyến khích di chuyển ứng dụng từ một nhóm tin tưởng được gán tự động sang một nhóm tin tưởng khác. Thay vào đó, bạn có thể sửa các quy tắc cho một ứng dụng riêng lẻ.

Để thay đổi nhóm tin tưởng mà ứng dụng đã được tự động gán bởi Kaspersky Endpoint Security khi ứng dụng khởi chạy lần đầu tiên:

1. Mở cửa sổ cấu hình ứng dụng.

2. Trong phần bên trái của cửa sổ, trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát Đặc quyền Ứng dụng**.

   Cấu hình của thành phần Kiểm soát Đặc quyền Ứng dụng sẽ được hiển thị ở phần bên phải của cửa sổ.

3. Nhấn nút **Ứng dụng**.

   Thẻ **Quy tắc quản lý ứng dụng** trong cửa sổ **Ứng dụng** sẽ được mở ra.

4. Chọn ứng dụng liên quan trên thẻ **Quy tắc quản lý ứng dụng**.

5. Thực hiện một trong các thao tác sau:

   - Phải chuột để hiển thị menu ngữ cảnh của ứng dụng. Trong menu ngữ cảnh của ứng dụng, chọn **Di chuyển đến nhóm** → <τ| ν νη ∫μ>.

- Để mở menu ngữ cảnh, nhấn vào liên kết **Tin tưởng** / **Hạn chế mức thấp** / **Hạn chế mức cao** / **Không Tin tưởng**. Trong menu ngữ cảnh, chọn nhóm tin tưởng được yêu cầu.

6. Nhấn **OK**.

7. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Chọn một nhóm tin tưởng cho các ứng dụng được khởi động trước Kaspersky Endpoint Security

Thành phần này chỉ kiểm soát hoạt động mạng của các ứng dụng đã được khởi động trước Kaspersky Endpoint Security. Tính năng kiểm soát được thực hiện thông qua các quy tắc mạng được quy định trong cấu hình Tường lửa. Để quy định các quy tắc mạng được áp dụng cho hoạt động mạng của những ứng dụng đó, bạn phải chọn một nhóm tin tưởng.

Để chọn nhóm tin tưởng cho các ứng dụng được khởi động trước Kaspersky Endpoint Security:

1. Mở cửa sổ cấu hình ứng dụng.

2. Trong phần bên trái của cửa sổ, trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát Đặc quyền Ứng dụng**.

   Cấu hình của thành phần Kiểm soát Đặc quyền Ứng dụng sẽ được hiển thị ở phần bên phải của cửa sổ.

3. Nhấn nút **Chỉnh sửa**.

   Việc này sẽ mở ra cửa sổ **Lựa chọn nhóm tin tưởng**.

4. Chọn nhóm tin tưởng cần thiết.

5. Nhấn **OK**.

6. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Quản lý quy tắc kiểm soát ứng dụng

Theo mặc định, hoạt động của ứng dụng được kiểm soát bởi các quy tắc kiểm soát ứng dụng được quy định cho nhóm tin tưởng đã được Kaspersky Endpoint Security gán ứng dụng vào đó khi khởi chạy nó lần đầu. Nếu cần, bạn có thể sửa các quy tắc kiểm soát ứng dụng cho cả một nhóm tin tưởng, cho một ứng dụng riêng lẻ, hoặc một nhóm các ứng dụng trong một nhóm tin tưởng.

Các quy tắc kiểm soát ứng dụng được quy định cho các ứng dụng riêng lẻ hoặc nhóm ứng dụng trong một nhóm tin tưởng có mức độ ưu tiên cao hơn các quy tắc kiểm soát ứng dụng được quy định cho một nhóm tin tưởng. Nói cách khác, nếu cấu hình quy tắc kiểm soát ứng dụng cho một ứng dụng riêng lẻ hoặc một nhóm các ứng dụng trong một nhóm tin tưởng khác với cấu hình quy tắc kiểm soát ứng dụng cho nhóm tin tưởng đó, thành phần Kiểm soát Đặc quyền Ứng dụng sẽ kiểm soát hoạt động của ứng dụng hoặc nhóm ứng dụng trong nhóm tin tưởng theo các quy tắc kiểm soát ứng dụng cho ứng dụng hoặc nhóm ứng dụng đó.

Thay đổi quy tắc kiểm soát ứng dụng cho các nhóm tin tưởng và nhóm ứng dụng

Các quy tắc kiểm soát ứng dụng tối ưu cho các nhóm tin tưởng khác nhau sẽ được tạo ở chế độ mặc định. Cấu hình của các quy tắc kiểm soát nhóm ứng dụng sẽ kế thừa giá trị từ cấu hình của các quy tắc kiểm soát nhóm tin tưởng. Bạn có thể sửa các quy tắc kiểm soát nhóm tin tưởng được thiết lập sẵn, cũng như các quy tắc để kiểm soát nhóm ứng dụng.

Để sửa các quy tắc kiểm soát nhóm tin tưởng hoặc các quy tắc để kiểm soát nhóm ứng dụng:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát Đặc quyền Ứng dụng**.

   Cấu hình của thành phần Kiểm soát Đặc quyền Ứng dụng sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Nhấn nút **Ứng dụng**.

   Việc này sẽ mở ra thẻ **Quy tắc quản lý ứng dụng** trong cửa sổ **Kiểm soát Đặc quyền Ứng dụng**.
4. Chọn nhóm tin tưởng hoặc nhóm ứng dụng cần thiết.
5. Từ menu ngữ cảnh của một nhóm tin tưởng hoặc nhóm ứng dụng, chọn **Quy tắc nhóm**.

   Cửa sổ **Quy tắc kiểm soát nhóm ứng dụng** sẽ được mở ra.
6. Trong cửa sổ **Quy tắc kiểm soát nhóm ứng dụng**, thực hiện một trong các thao tác sau:

   - Để sửa các quy tắc kiểm soát nhóm tin tưởng hoặc quy tắc kiểm soát nhóm ứng dụng quy định các quyền của nhóm tin tưởng hoặc nhóm ứng dụng trong việc truy cập đến registry hệ điều hành, tập tin người dùng và cấu hình ứng dụng, chọn thẻ **Tập tin và hệ thống registry**.
   - Để sửa các quy tắc kiểm soát nhóm tin tưởng hoặc quy tắc kiểm soát nhóm ứng dụng quy định các quyền của nhóm tin tưởng hoặc nhóm ứng dụng trong việc truy cập đến các tiến trình và đối tượng của hệ điều hành, chọn thẻ **Quyền**.
7. Ở tài nguyên cần thiết, trong cột của hành động tương ứng, nhấn phải chuột để mở ra menu ngữ cảnh.
8. Từ menu ngữ cảnh, chọn đề mục cần thiết.

   - **Kế thừa**
   - **Cho phép**
   - **Ngăn chặn**
   - **Báo cáo sự kiện**

   Nếu bạn đang sửa các quy tắc kiểm soát nhóm tin tưởng, đề mục **Kế thừa** sẽ không khả dụng.
9. Nhấn **OK**.

10. Trong cửa sổ **Ứng dụng**, nhấn **OK**.

11. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Sửa một quy tắc kiểm soát ứng dụng

Theo mặc định, cấu hình quy tắc kiểm soát ứng dụng của các ứng dụng thuộc một nhóm ứng dụng hoặc nhóm tin tưởng sẽ kế thừa giá trị của cấu hình quy tắc kiểm soát nhóm tin tưởng. Bạn có thể sửa cấu hình của các quy tắc kiểm soát ứng dụng.

Để thay đổi một quy tắc kiểm soát ứng dụng:

1. Mở cửa sổ cấu hình ứng dụng.

2. Trong phần bên trái của cửa sổ, trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát Đặc quyền Ứng dụng**.

   Cấu hình của thành phần Kiểm soát Đặc quyền Ứng dụng sẽ được hiển thị ở phần bên phải của cửa sổ.

3. Nhấn nút **Ứng dụng**.

   Việc này sẽ mở ra thẻ **Quy tắc quản lý ứng dụng** trong cửa sổ **Kiểm soát Đặc quyền Ứng dụng**.

4. Chọn ứng dụng cần thiết.

5. Thực hiện một trong các thao tác sau:

   - Từ menu ngữ cảnh của ứng dụng, chọn **Quy tắc ứng dụng**.
   - Nhấn nút **Bổ sung** ở góc phải dưới của thẻ **Quy tắc quản lý ứng dụng**.

   Cửa sổ **Quy tắc quản lý ứng dụng** sẽ được mở ra.

6. Trong cửa sổ **Quy tắc quản lý ứng dụng**, thực hiện một trong các thao tác sau:

   - Để sửa các quy tắc kiểm soát ứng dụng quy định các quyền của ứng dụng trong việc truy cập đến registry hệ điều hành, tập tin người dùng và cấu hình ứng dụng, chọn thẻ **Tập tin và hệ thống registry**.
   - Để sửa các quy tắc kiểm soát ứng dụng quy định các quyền của ứng dụng trong việc truy cập đến các tiến trình và đối tượng của hệ điều hành, chọn thẻ **Quyền**.

7. Ở tài nguyên cần thiết, trong cột của hành động tương ứng, nhấn phải chuột để mở ra menu ngữ cảnh.

8. Từ menu ngữ cảnh, chọn đề mục cần thiết.

   - **Kế thừa**
   - **Cho phép**
   - **Ngăn chặn**
   - **Báo cáo sự kiện**

9. Nhấn **OK**.

10. Trong cửa sổ **Ứng dụng**, nhấn **OK**.

11. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Tắt tính năng tải về và cập nhật quy tắc kiểm soát ứng dụng từ cơ sở dữ liệu Kaspersky Security Network

Theo mặc định, khi thông tin mới về một ứng dụng được phát hiện trong cơ sở dữ liệu Kaspersky Security Network, Kaspersky Endpoint Security sẽ áp dụng các quy tắc kiểm soát được tải về từ cơ sở dữ liệu KSN cho ứng dụng này. Bạn có thể sửa thủ công các quy tắc kiểm soát cho ứng dụng.

Nếu một ứng dụng không nằm trong cơ sở dữ liệu Kaspersky Security Network khi được khởi chạy lần đầu tiên, nhưng thông tin về nó đã được thêm vào cơ sở dữ liệu sau đó, theo mặc định Kaspersky Endpoint Security sẽ tự động cập nhật quy tắc kiểm soát cho ứng dụng này.

Bạn có thể tắt tính năng tải về các quy tắc kiểm soát ứng dụng từ cơ sở dữ liệu Kaspersky Security Network và tự động cập nhật các quy tắc kiểm soát cho những ứng dụng không xác định trước đó .

Để tắt tính năng tải về và cập nhật quy tắc kiểm soát ứng dụng từ cơ sở dữ liệu Kaspersky Security Network:

1. Mở cửa sổ cấu hình ứng dụng.

2. Trong phần bên trái của cửa sổ, trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát Đặc quyền Ứng dụng**.

   Cấu hình của thành phần Kiểm soát Đặc quyền Ứng dụng sẽ được hiển thị ở phần bên phải của cửa sổ.

3. Xóa hộp kiểm **Cập nhật các quy tắc quản lý cho những chương trình chưa biết trước đây từ cơ sở dữ liệu KSN**.

4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Tắt việc kế thừa các hạn chế từ tiến trình cha

Việc khởi động ứng dụng có thể được bắt đầu bởi người dùng hoặc một ứng dụng đang chạy khác. Khi ứng dụng được khởi động bởi một ứng dụng khác, một chuỗi khởi động sẽ được tạo, bao gồm các tiến trình cha và con.

Khi một ứng dụng cố gắng nhận quyền truy cập đến một tài nguyên được bảo vệ, Kiểm soát Đặc quyền Ứng dụng sẽ phân tích tất cả các tiến trình cha của ứng dụng để xác định liệu các tiến trình này có quyền truy cập đến tài nguyên được bảo vệ hay không. Quy tắc ưu tiên tối thiểu sau đó sẽ được tuân thủ: khi so sánh quyền truy cập của ứng dụng đến quyền của các tiến trình cha, quyền truy cập với ưu tiên tối thiểu sẽ được áp dụng cho hoạt động của ứng dụng.

Mức độ ưu tiên của các quyền truy cập là như sau:

1. **Cho phép** Quyền truy cập này có mức độ ưu tiên cao nhất.

2. **Ngăn chặn** Quyền truy cập này có mức độ ưu tiên thấp nhất.

Cơ cấu này nhằm ngăn một ứng dụng không tin tưởng hoặc một ứng dụng có quyền bị hạn chế khỏi việc sử dụng một ứng dụng được tin tưởng để thực hiện các hành động yêu cầu một số đặc quyền nhất định.

Nếu hoạt động của một ứng dụng bị chặn do thiếu quyền được cấp cho tiến trình cha, bạn có thể sửa các quyền này hoặc tắt tính kế thừa hạn chế từ tiến trình cha.

Để tắt việc kế thừa các hạn chế từ tiến trình cha:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát Đặc quyền Ứng dụng**.

   Cấu hình của thành phần Kiểm soát Đặc quyền Ứng dụng sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Nhấn nút **Ứng dụng**.

   Việc này sẽ mở ra thẻ **Quy tắc quản lý ứng dụng** trong cửa sổ **Kiểm soát Đặc quyền Ứng dụng**.
4. Chọn ứng dụng cần thiết.
5. Từ menu ngữ cảnh của ứng dụng, chọn **Quy tắc ứng dụng**.

   Cửa sổ **Quy tắc quản lý ứng dụng** sẽ được mở ra.
6. Trong cửa sổ **Quy tắc quản lý ứng dụng**, chọn thẻ **Loại trừ**.
7. Chọn hộp kiểm **Không kế thừa những hạn chế của tiến trình cha (ứng dụng)**.
8. Nhấn **OK**.
9. Trong cửa sổ **Ứng dụng**, nhấn **OK**.
10. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Loại trừ các hành động của ứng dụng cụ thể khỏi quy tắc kiểm soát ứng dụng

Để loại trừ các hành động của ứng dụng cụ thể khỏi quy tắc kiểm soát ứng dụng:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát Đặc quyền Ứng dụng**.

   Cấu hình của thành phần Kiểm soát Đặc quyền Ứng dụng sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Nhấn nút **Ứng dụng**.

   Việc này sẽ mở ra thẻ **Quy tắc quản lý ứng dụng** trong cửa sổ **Kiểm soát Đặc quyền Ứng dụng**.
4. Chọn ứng dụng cần thiết.

5. Từ menu ngữ cảnh của ứng dụng, chọn **Quy tắc ứng dụng**.

   Cửa sổ **Quy tắc quản lý ứng dụng** sẽ được mở ra.

6. Chọn thẻ **Loại trừ**.

7. Chọn hộp kiểm cạnh các hành động ứng dụng không cần được giám sát.

8. Nhấn **OK**.

9. Trong cửa sổ **Ứng dụng**, nhấn **OK**.

10. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Xóa các quy tắc kiểm soát ứng dụng đã lỗi thời

Theo mặc định, các quy tắc kiểm soát cho ứng dụng chưa được khởi động trong 60 ngày đều được xóa tự động. Bạn có thể thay đổi thời gian lưu trữ các quy tắc kiểm soát cho các ứng dụng không được sử dụng, hoặc tắt tính năng tự động xóa các quy tắc.

Để xóa các quy tắc kiểm soát ứng dụng đã lỗi thời:

1. Mở cửa sổ cấu hình ứng dụng.

2. Trong phần bên trái của cửa sổ, trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát Đặc quyền Ứng dụng**.

   Cấu hình của thành phần Kiểm soát Đặc quyền Ứng dụng sẽ được hiển thị ở phần bên phải của cửa sổ.

3. Thực hiện một trong các thao tác sau:

   - Nếu bạn muốn Kaspersky Endpoint Security xóa quy tắc kiểm soát cho các ứng dụng không được sử dụng, chọn hộp kiểm **Xóa các quy tắc của những chương trình đã không thực thi nhiều hơn** và quy định số ngày tương ứng.

   - Để tắt tính năng tự động xóa quy tắc kiểm soát cho các ứng dụng không được sử dụng, xóa hộp kiểm **Xóa các quy tắc của những chương trình đã không thực thi nhiều hơn**.

4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Bảo vệ tài nguyên hệ điều hành và dữ liệu danh tính

Kiểm soát Đặc quyền Ứng dụng có chức năng quản lý các quyền của ứng dụng trong việc thực hiện hành động đối với nhiều hạng mục tài nguyên hệ điều hành và dữ liệu danh tính.

Các chuyên gia Kaspersky đã thiết lập sẵn các hạng mục tài nguyên được bảo vệ. Bạn không thể sửa hoặc xóa các hạng mục tài nguyên được bảo vệ được thiết lập sẵn hoặc tài nguyên được bảo vệ nằm trong các hạng mục này.

Bạn có thể thực hiện các hành động sau:

- Bổ sung một hạng mục tài nguyên được bảo vệ mới.
- Bổ sung một tài nguyên được bảo vệ mới.
- Tắt tính năng bảo vệ một tài nguyên.

Bổ sung một hạng mục tài nguyên được bảo vệ

Để bổ sung một hạng mục tài nguyên được bảo vệ mới:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát Đặc quyền Ứng dụng**.

   Cấu hình của thành phần Kiểm soát Đặc quyền Ứng dụng sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Nhấn nút **Tài nguyên**.

   Việc này sẽ mở ra thẻ **Bảo vệ tài nguyên** trong cửa sổ **Kiểm soát Đặc quyền Ứng dụng**.
4. Ở phần bên trái của thẻ **Bảo vệ tài nguyên**, chọn một mục hoặc hạng mục tài nguyên được bảo vệ để bổ sung một hạng mục tài nguyên được bảo vệ.
5. Nhấn nút **Thêm**, và trong danh sách thả xuống chọn **Danh mục**.

   Cửa sổ **Danh mục tài nguyên được bảo vệ** sẽ được mở ra.
6. Trong cửa sổ **Danh mục tài nguyên được bảo vệ** được mở ra, nhập tên cho hạng mục tài nguyên được bảo vệ mới.
7. Nhấn **OK**.

   Một đề mục mới sẽ xuất hiện trong danh sách các hạng mục tài nguyên được bảo vệ.
8. Trong cửa sổ **Kiểm soát Đặc quyền Ứng dụng**, nhấn **OK**.
9. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Sau khi bạn thêm một hạng mục tài nguyên được bảo vệ, bạn có thể sửa hoặc xóa nó bằng cách nhấn nút **Chỉnh sửa** hoặc **Gỡ bỏ** ở góc trên bên trái của thẻ **Bảo vệ tài nguyên**.

Bổ sung một tài nguyên được bảo vệ

Để bổ sung một tài nguyên được bảo vệ:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát Đặc quyền Ứng dụng**.

Cấu hình của thành phần Kiểm soát Đặc quyền Ứng dụng sẽ được hiển thị ở phần bên phải của cửa sổ.

3. Nhấn nút **Tài nguyên**.

   Việc này sẽ mở ra thẻ **Bảo vệ tài nguyên** trong cửa sổ **Kiểm soát Đặc quyền Ứng dụng**.

4. Ở phần bên trái của thẻ **Bảo vệ tài nguyên**, chọn một mục hoặc hạng mục tài nguyên được bảo vệ để bổ sung một tài nguyên được bảo vệ mới.

5. Nhấn nút **Thêm**, và trong danh sách thả xuống chọn loại tài nguyên mà bạn muốn bổ sung:

   - **Tập tin hoặc thư mục**.
   - **Khóa registry**.

   Cửa sổ **Bảo vệ tài nguyên** sẽ được mở ra.

6. Trong cửa sổ **Bảo vệ tài nguyên**, nhập tên của tài nguyên được bảo vệ vào trường **Tên**.

7. Nhấn nút **Duyệt**.

8. Trong cửa sổ được mở ra, nhập cấu hình cần thiết tùy thuộc vào kiểu tài nguyên được bảo vệ mà bạn muốn bổ sung. Nhấn **OK**.

9. Trong cửa sổ **Bảo vệ tài nguyên**, nhấn **OK**.

   Một đề mục mới sẽ xuất hiện trong danh sách các tài nguyên được bảo vệ thuộc hạng được chọn trên thẻ **Bảo vệ tài nguyên**.

10. Trong cửa sổ **Kiểm soát Đặc quyền Ứng dụng**, nhấn **OK**.

11. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Sau khi bạn thêm một tài nguyên được bảo vệ, bạn có thể sửa hoặc xóa nó bằng cách nhấn nút **Chỉnh sửa** hoặc **Gỡ bỏ** ở góc trên bên trái của thẻ **Bảo vệ tài nguyên**.

Tắt tính năng bảo vệ tài nguyên

Để tắt tính năng bảo vệ tài nguyên:

1. Mở cửa sổ cấu hình ứng dụng.

2. Trong phần bên trái của cửa sổ, trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát Đặc quyền Ứng dụng**.

   Cấu hình của thành phần Kiểm soát Đặc quyền Ứng dụng sẽ được hiển thị ở phần bên phải của cửa sổ.

3. Ở phía bên phải của cửa sổ, bấm vào nút **Tài nguyên**.

   Việc này sẽ mở ra thẻ **Bảo vệ tài nguyên** trong cửa sổ **Kiểm soát Đặc quyền Ứng dụng**.

4. Thực hiện một trong các thao tác sau:

- Ở phần bên trái của thẻ, trong danh sách các tài nguyên được bảo vệ, chọn tài nguyên mà bạn muốn tắt bảo vệ và xóa hộp kiểm cạnh tên nó.

- Nhấn **Loại trừ** và làm như sau:

  a. Trong cửa sổ **Loại trừ** được mở ra, nhấp vào nút **Thêm**. Trong danh sách thả xuống, chọn loại tài nguyên mà bạn muốn bổ sung vào danh sách loại trừ khỏi tính năng bảo vệ của thành phần Kiểm soát Đặc quyền Ứng dụng: **Tập tin hoặc thư mục** hay **Khóa registry**.

  Cửa sổ **Bảo vệ tài nguyên** sẽ được mở ra.

  b. Trong cửa sổ **Bảo vệ tài nguyên**, nhập tên của tài nguyên được bảo vệ vào trường **Tên**.

  c. Nhấn nút **Duyệt**.

  d. Trong cửa sổ được mở ra, nhập cấu hình cần thiết tùy thuộc vào kiểu tài nguyên được bảo vệ mà bạn muốn bổ sung vào danh sách loại trừ khỏi tính năng bảo vệ của thành phần Kiểm soát Đặc quyền Ứng dụng.

  e. Nhấn **OK**.

  f. Trong cửa sổ **Bảo vệ tài nguyên**, nhấn **OK**.

  Một yếu tố mới sẽ xuất hiện trong danh sách các tài nguyên được loại trừ khỏi tính năng bảo vệ của thành phần Kiểm soát Đặc quyền Ứng dụng.

  > Sau bổ sung một tài nguyên vào danh sách loại trừ khỏi tính năng bảo vệ của thành phần Kiểm soát Đặc quyền Ứng dụng, bạn có thể sửa hoặc xóa nó bằng cách nhấn nút **Chỉnh sửa** hoặc **Gỡ bỏ** ở góc trên bên trái của thẻ **Loại trừ**.

  g. Trong cửa sổ **Loại trừ**, nhấn **OK**.

5. Trong cửa sổ **Kiểm soát Đặc quyền Ứng dụng**, nhấn **OK**.

6. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Giám sát Lỗ hổng Bảo mật

Thành phần này có thể được sử dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Microsoft Windows cho máy trạm. Thành phần này không thể được sử dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Microsoft Windows cho Máy chủ Tập tin.

Mục này chứa thông tin về Giám sát Lỗ hổng bảo mật và chỉ dẫn cách để bật hoặc tắt thành phần này.

Thông tin về Giám sát Lỗ hổng Bảo mật

Thành phần Giám sát Lỗ hổng bảo mật chạy tác vụ quét lỗ hổng bảo mật trong thời gian thực cho các ứng dụng đang chạy trên máy tính của người dùng và được khởi chạy bởi người dùng. Khi thành phần Giám sát Lỗ hổng bảo mật được bật, bạn sẽ không cần bắt đầu tác vụ Quét lỗ hổng bảo mật. Tác vụ Quét lỗ hổng bảo mật chỉ là cần thiết khi tác vụ quét này cho các ứng dụng được cài đặt trên máy tính của người dùng chưa từng được thực hiện, hoặc đã được thực hiện từ rất lâu rồi.

Bật và tắt Giám sát Lỗ hổng bảo mật

Thành phần Giám sát Lỗ hổng bảo mật bị tắt theo mặc định. Bạn có thể bật Giám sát Lỗ hổng bảo mật nếu cần thiết.

Có hai cách để bật hoặc tắt thành phần này:

- Trên thẻ **Bảo vệ và Kiểm soát** của cửa sổ chính của ứng dụng
- Từ cửa sổ cấu hình ứng dụng.

Để bật hoặc tắt Giám sát Lỗ hổng bảo mật trên thẻ Bảo vệ và Kiểm soát của cửa sổ chính của ứng dụng:

1. Mở cửa sổ chính của ứng dụng.
2. Chọn thẻ **Bảo vệ và Kiểm soát**.
3. Nhấn vào mục **Bảng kiểm soát**.
   Mục **Bảng kiểm soát** sẽ được mở ra.
4. Nhấn phải chuột để hiển thị menu ngữ cảnh của dòng có chứa thông tin về thành phần Giám sát Lỗ hổng bảo mật.
   Một menu để chọn hành động đối với thành phần sẽ được mở ra.
5. Thực hiện một trong các thao tác sau:
   - Để bật Giám sát Lỗ hổng bảo mật, chọn **Bắt đầu**.
     Biểu tượng trạng thái của thành phần , được hiển thị ở bên trái của dòng **Giám sát Lỗ hổng bảo mật** sẽ được chuyển sang biểu tượng .
   - Để tắt Giám sát Lỗ hổng bảo mật, chọn **Dừng**.

Biểu tượng trạng thái của thành phần , được hiển thị ở bên trái của dòng **Giám sát Lỗ hổng bảo mật** sẽ được chuyển sang biểu tượng .

Để bật hoặc tắt Giám sát Lỗ hổng bảo mật từ cửa sổ cấu hình ứng dụng:

1. Mở cửa sổ cấu hình ứng dụng.
2. Ở phần bên trái của cửa sổ, trong mục **Bảng kiểm soát**, chọn **Giám sát Lỗ hổng bảo mật**.
   Ở phần bên phải của cửa sổ, cấu hình của thành phần Giám sát Lỗ hổng bảo mật sẽ được hiển thị.
3. Trong phần bên phải của cửa sổ, thực hiện một trong các thao tác sau:
   - Nếu bạn muốn Kaspersky Endpoint Security bắt đầu quét lỗ hổng bảo mật cho các ứng dụng được khởi chạy, hoặc đang chạy trên máy tính của người dùng, chọn hộp kiểm **Cho phép giám sát lỗ hổng bảo mật**.
   - Nếu bạn không muốn Kaspersky Endpoint Security quét lỗ hổng bảo mật cho các ứng dụng được khởi chạy, hoặc đang chạy trên máy tính của người dùng, xóa hộp kiểm **Cho phép giám sát lỗ hổng bảo mật**.
4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Kiểm soát Thiết bị

Thành phần này có thể được sử dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Microsoft Windows cho máy trạm. Thành phần này không thể được sử dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Microsoft Windows cho máy chủ tập tin.

Mục này chứa thông tin về Kiểm soát Thiết bị và chỉ dẫn cách để thiết lập cấu hình thành phần.

Thông tin về Kiểm soát Thiết bị

Kiểm soát Thiết bị đảm bảo tính bảo mật của dữ liệu bí mật bằng cách hạn chế truy cập của người dùng đến các thiết bị được cài đặt trên máy tính hoặc kết nối đến máy tính, bao gồm:

- Thiết bị lưu trữ dữ liệu (ổ cứng, ổ đĩa di động, ổ băng, ổ đĩa CD/DVD)
- Công cụ truyền tải dữ liệu (modem, card mạng bên ngoài)
- Các thiết bị được thiết kế để chuyển dữ liệu thành các bản sao cứng (máy in)
- Bus kết nối (còn được gọi đơn giản là "bus"), là giao diện để kết nối các thiết bị đến máy tính (ví dụ như USB, FireWire, và Hồng ngoại)

Kiểm soát Thiết bị kiểm soát quyền truy cập của người dùng đến các thiết bị bằng cách áp dụng *quy tắc truy cập thiết bị* (còn được gọi là "quy tắc truy cập") và *quy tắc truy cập bus kết nối* (còn được gọi là "quy tắc truy cập bus").

Bật và tắt Kiểm soát Thiết bị

Theo mặc định, Kiểm soát Thiết bị sẽ được bật. Bạn có thể tắt Kiểm soát Thiết bị nếu cần thiết.

Có hai cách để bật hoặc tắt thành phần này:

- Trên thẻ **Bảo vệ và Kiểm soát** của cửa sổ chính của ứng dụng
- Từ cửa sổ cấu hình ứng dụng.

*Để bật hoặc tắt Kiểm soát Thiết bị trên thẻ **Bảo vệ và Kiểm soát** của cửa sổ chính của ứng dụng:*

1. Mở cửa sổ chính của ứng dụng.
2. Chọn thẻ **Bảo vệ và Kiểm soát**.
3. Nhấn vào mục **Bảng kiểm soát**.
   Mục **Bảng kiểm soát** sẽ được mở ra.
4. Nhấn phải chuột để gọi menu ngữ cảnh của dòng có chứa thông tin về thành phần Kiểm soát Thiết bị.
   Một menu để chọn hành động đối với thành phần sẽ được mở ra.

5. Thực hiện một trong các thao tác sau:

   - Để bật Kiểm soát Thiết bị, chọn **Bắt đầu** trong menu.
   - Để tắt Kiểm soát Thiết bị, chọn **Dừng** trong menu.

Để bật hoặc tắt Kiểm soát Thiết bị từ cửa sổ cấu hình ứng dụng:

1. Mở cửa sổ cấu hình ứng dụng.
2. Ở phần bên trái của cửa sổ, trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát Thiết bị**.
   Ở phần bên phải của cửa sổ, cấu hình của thành phần Kiểm soát Thiết bị sẽ được hiển thị.
3. Thực hiện một trong các thao tác sau:
   - Nếu bạn muốn bật Kiểm soát Thiết bị, chọn hộp kiểm **Bật Kiểm soát Thiết bị**.
   - Nếu bạn muốn tắt Kiểm soát Thiết bị, xóa hộp kiểm **Bật Kiểm soát Thiết bị**.
4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Thông tin về quy tắc truy cập đến các thiết bị và bus kết nối

Một quy tắc truy cập thiết bị là một tổ hợp các tham số quy định các chức năng sau đây của thành phần Kiểm soát Thiết bị:

- Cho phép những người dùng và / hoặc nhóm người dùng được chọn truy cập các loại thiết bị cụ thể trong các khoảng thời gian cụ thể.
  Bạn có thể chọn một người dùng và / hoặc nhóm người dùng và tạo một lịch truy cập thiết bị cho họ.
- Đặt quyền để đọc nội dung của các thiết bị bộ nhớ.
- Đặt quyền để sửa nội dung của các thiết bị bộ nhớ.

Theo mặc định, quyền truy cập sẽ được tạo cho tất cả các loại thiết bị trong phân loại của thành phần Kiểm soát Thiết bị. Các quy tắc đó sẽ cho phép người dùng toàn quyền truy cập đến thiết bị vào mọi thời điểm, nếu quyền truy cập đến các bus kết nối của loại thiết bị tương ứng là được cho phép.

Quy tắc truy cập bus kết nối cho phép hoặc chặn truy cập đến bus kết nối.

Các quy tắc cho phép truy cập đến bus theo mặc định sẽ được tạo cho tất cả các bus kết nối có trong phân loại của thành phần Kiểm soát Thiết bị.

Bạn không thể tạo hoặc xóa các quy tắc truy cập thiết bị hoặc quy tắc truy cập bus kết nối; bạn chỉ có thể sửa chúng.

Thông tin về các thiết bị được tin tưởng

Thiết bị được tin tưởng là các thiết bị mà những người dùng được quy định trong cấu hình thiết bị được tin tưởng có thể truy cập vào bất cứ lúc nào.

Các hành động sau có thể được thực hiện khi làm việc với các thiết bị được tin tưởng:

- Thêm thiết bị vào danh sách các thiết bị được tin tưởng.
- Thay đổi người dùng và / hoặc nhóm người dùng được phép truy cập thiết bị được tin tưởng.
- Xóa thiết bị khỏi danh sách các thiết bị được tin tưởng.

Nếu bạn đã thêm một thiết bị vào danh sách các thiết bị được tin tưởng và tạo một quy tắc chặn hoặc hạn chế truy cập cho loại thiết bị này, Kaspersky Endpoint Security sẽ quyết định có nên cấp quyền truy cập đến thiết bị hay không dựa vào việc nó có tên hay không trong danh sách các thiết bị được tin tưởng. Việc có tên trong danh sách các thiết bị được tin tưởng sẽ có ưu tiên cao hơn so với một quy tắc truy cập.

Quyết định tiêu chuẩn khi truy cập thiết bị

Kaspersky Endpoint Security sẽ đưa ra quyết định về việc cho phép truy cập đến một thiết bị sau khi người dùng đã kết nối thiết bị đến máy tính.

Quyết định tiêu chuẩn khi truy cập thiết bị

Không.	Điều kiện ban đầu	Các bước trung gian cần thực hiện cho đến khi quyết định về việc truy cập đến thiết bị được đưa ra			Quyết định khi truy cập thiết bị
		Kiểm tra xem thiết bị có được bao gồm trong danh sách các thiết bị được tin tưởng hay không	Kiểm tra truy cập đến thiết bị dựa trên quy tắc truy cập	Kiểm tra truy cập đến bus dựa trên quy tắc truy cập bus	
1	Thiết bị không có trong phân loại thiết bị của thành phần Kiểm soát Thiết bị.	Không được bao gồm trong danh sách các thiết bị được tin tưởng.	Không có quy tắc truy cập.	Không được quét.	Cho phép truy cập.
2	Thiết bị được tin tưởng.	Được bao gồm trong danh sách các thiết bị được tin tưởng.	Không được quét.	Không được quét.	Cho phép truy cập.
3	Cho phép truy cập đến thiết bị.	Không được bao gồm trong danh sách các thiết bị được tin tưởng.	Cho phép truy cập.	Không được quét.	Cho phép truy cập.
4	Việc truy cập đến thiết bị tùy thuộc vào bus.	Không được bao gồm trong danh sách các thiết bị được tin tưởng.	Việc truy cập tùy thuộc vào bus.	Cho phép truy cập.	Cho phép truy cập.

5	Việc truy cập đến thiết bị tùy thuộc vào bus.	Không được bao gồm trong danh sách các thiết bị được tin tưởng.	Việc truy cập tùy thuộc vào bus.	Truy cập bị chặn.	Truy cập bị chặn.
6	Cho phép truy cập đến thiết bị. Không tìm thấy quy tắc truy cập bus nào.	Không được bao gồm trong danh sách các thiết bị được tin tưởng.	Cho phép truy cập.	Không có quy tắc truy cập bus nào.	Cho phép truy cập.
7	Chặn truy cập đến thiết bị.	Không được bao gồm trong danh sách các thiết bị được tin tưởng.	Truy cập bị chặn.	Không được quét.	Truy cập bị chặn.
8	Không tìm thấy quy tắc truy cập thiết bị hay quy tắc truy cập bus nào.	Không được bao gồm trong danh sách các thiết bị được tin tưởng.	Không có quy tắc truy cập.	Không có quy tắc truy cập bus nào.	Cho phép truy cập.
9	Không có quy tắc truy cập thiết bị nào.	Không được bao gồm trong danh sách các thiết bị được tin tưởng.	Không có quy tắc truy cập.	Cho phép truy cập.	Cho phép truy cập.
10	Không có quy tắc truy cập thiết bị nào.	Không được bao gồm trong danh sách các thiết bị được tin tưởng.	Không có quy tắc truy cập.	Truy cập bị chặn.	Truy cập bị chặn.

Bạn có thể sửa quy tắc truy cập thiết bị sau khi kết nối thiết bị. Nếu thiết bị được kết nối và quy tắc truy cập cho phép truy cập đến thiết bị này, bạn có thể sửa quy tắc truy cập và quy tắc chặn, Kaspersky Endpoint Security sẽ chặn truy cập khi có bất kỳ hoạt động tập tin nào được yêu cầu từ thiết bị sau đó (xem cây thư mục, đọc, ghi). Một thiết bị không có hệ thống tập tin sẽ chỉ bị chặn ở lần tiếp theo thiết bị này được kết nối.

Nếu một người dùng của máy tính có cài đặt Kaspersky Endpoint Security phải yêu cầu truy cập đến một thiết bị mà người dùng đó tin là đã bị chặn do nhầm lẫn, hãy gửi cho người dùng đó hướng dẫn yêu cầu truy cập.

Sửa đổi một quy tắc truy cập thiết bị

Tùy thuộc vào loại thiết bị, bạn có thể sửa đổi các cấu hình truy cập khác nhau, ví dụ như danh sách người dùng được truy cập thiết bị, lịch truy cập, và cho phép / chặn truy cập.

Để sửa đổi một quy tắc truy cập thiết bị:

1. Mở cửa sổ cấu hình ứng dụng.
2. Ở phần bên trái của cửa sổ, trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát Thiết bị**.
   Ở phần bên phải của cửa sổ, cấu hình của thành phần Kiểm soát Thiết bị sẽ được hiển thị.
3. Ở phần bên phải của cửa sổ, chọn thẻ **Các loại thiết bị**.

Thẻ **Các loại thiết bị** chứa quy tắc truy cập cho tất cả các thiết bị được bao gồm trong phân loại của thành phần Kiểm soát Thiết bị.

4. Chọn quy tắc truy cập mà bạn muốn sửa.

5. Nhấn nút **Chỉnh sửa**. Nút này chỉ có thể được sử dụng cho các loại thiết bị có một hệ thống tập tin.

   Cửa sổ **Cấu hình quy tắc truy xuất thiết bị** sẽ được mở ra.

   Theo mặc định, một quy tắc truy cập thiết bị cho phép tất cả người dùng quyền truy cập toàn diện vào loại thiết bị được quy định vào bất cứ thời điểm nào. Trong danh sách **Người dùng và / hoặc nhóm người dùng**, quy tắc truy cập này chứa nhóm **Tất cả**. Trong bảng **Cấu hình lịch và quyền truy cập**, quy tắc truy cập này chứa **Lịch mặc định** để truy cập các thiết bị, với quyền thực hiện mọi loại thao tác với thiết bị.

6. Sửa cấu hình của quy tắc truy cập thiết bị:

   a. Chọn một người dùng và / hoặc nhóm người dùng từ danh sách **Người dùng và / hoặc nhóm người dùng**.

      Để sửa danh sách **Người dùng và / hoặc nhóm người dùng**, sử dụng các nút **Thêm**, **Chỉnh sửa** và **Gỡ bỏ**.

   b. Trong bảng **Cấu hình lịch và quyền truy cập**, thiết lập lịch truy cập các thiết bị cho người dùng và / hoặc nhóm người dùng được lựa chọn. Để làm điều này, chọn các hộp kiểm cạnh tên của lịch truy cập cho các thiết bị mà bạn muốn sử dụng trong quy tắc truy cập thiết bị sẽ được sửa.

      Để sửa danh sách lịch truy cập thiết bị, sử dụng các nút **Tạo**, **Chỉnh sửa**, **Sao chép** và **Gỡ bỏ** trong bảng **Cấu hình lịch và quyền truy cập**.

   c. Cho từng lịch truy cập thiết bị được sử dụng trong quy tắc được sửa, quy định hoạt động được cho phép khi làm việc với các thiết bị. Để làm điều này, trong bảng **Cấu hình lịch và quyền truy cập**, chọn các hộp kiểm trong cột chứa tên của hoạt động tương ứng.

   d. Nhấn **OK**.

   Sau khi bạn đã sửa cấu hình mặc định của quy tắc truy cập thiết bị, cấu hình truy cập đến loại thiết bị trong cột **Truy cập** của bảng trên thẻ **Các loại thiết bị** sẽ được chuyển sang giá trị *Giới hạn bởi các quy tắc*.

7. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Bổ sung hoặc loại trừ các bản ghi trong nhật ký sự kiện

Nhật ký sự kiện chỉ khả dụng cho các hoạt động với tập tin trên ổ đĩa di động.

Để bật hoặc tắt nhật ký sự kiện:

1. Mở cửa sổ cấu hình ứng dụng.

2. Ở phần bên trái của cửa sổ, trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát Thiết bị**.

   Ở phần bên phải của cửa sổ, cấu hình của thành phần Kiểm soát Thiết bị sẽ được hiển thị.

3. Ở phần bên phải của cửa sổ, chọn thẻ **Các loại thiết bị**.

Thẻ **Các loại thiết bị** chứa quy tắc truy cập cho tất cả các thiết bị được bao gồm trong phân loại của thành phần Kiểm soát Thiết bị.

4. Chọn **Ổ đĩa di động** trong bảng thiết bị.

   Nút **Nhật ký** sẽ có thể được sử dụng ở phần trên của bảng.

5. Nhấn nút **Nhật ký**.

   Việc này sẽ mở ra cửa sổ **Cấu hình Nhật ký**.

6. Thực hiện một trong các thao tác sau:

   - Nếu bạn muốn ghi lại các hoạt động xóa và ghi tập tin trên ổ đĩa di động, chọn hộp kiểm **Cho phép ghi nhật ký**.

     Kaspersky Endpoint Security sẽ lưu một sự kiện đến tập tin nhật ký và gửi một thông báo đến Máy chủ Quản trị của Kaspersky Security Center mỗi khi người dùng thực hiện hoạt động ghi hoặc xóa với các tập tin trên ổ đĩa di động.

   - Nếu không, hãy xóa hộp kiểm **Cho phép ghi nhật ký**.

7. Quy định các hành động cần được ghi lại. Để làm điều này, thực hiện một trong các hành động sau:

   - Nếu bạn muốn Kaspersky Endpoint Security ghi lại tất cả các sự kiện, chọn hộp kiểm **Lưu thông tin về tất cả các tập tin**.

   - Nếu bạn muốn Kaspersky Endpoint Security chỉ ghi lại thông tin về các sự kiện của một định dạng nhất định, trong mục **Bộ lọc định dạng tập tin**, chọn hộp kiểm đối diện các định dạng tập tin liên quan.

8. Quy định các hành động của người dùng Kaspersky Endpoint Security phải được ghi lại như các sự kiện. Để làm điều này:

   a. Trong mục **Người dùng**, nhấn nút **Lựa chọn**.

      Cửa sổ **Chọn Người dùng hoặc Nhóm Người dùng** tiêu chuẩn trong Microsoft Windows sẽ được mở ra.

   b. Nhập hoặc sửa danh sách người dùng và / hoặc nhóm người dùng.

   Khi người dùng được quy định trong mục **Người dùng** ghi lên các tập tin đặt trên ổ đĩa di động, hoặc xóa tập tin từ ổ di động, Kaspersky Endpoint Security sẽ lưu thông tin về các hoạt động đó đến nhật ký sự kiện và gửi một thông báo đến Máy chủ Quản trị của Kaspersky Security Center.

9. Trong cửa sổ **Cấu hình Nhật ký**, nhấn **OK**.

10. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Bạn có thể xem các sự kiện liên quan với các tập tin trên các ổ đĩa di động trong Bảng Điều khiển Quản trị Kaspersky Security Center trong không gian làm việc của nút **Máy chủ Quản trị** trên thẻ **Sự kiện**. Để các sự kiện được hiển thị trong bản ghi sự kiện Kaspersky Endpoint Security cục bộ, bạn phải chọn hộp kiểm **Thao tác với tập tin đã được thực thi** trong thiết lập thông báo cho thành phần Kiểm soát Thiết bị.

Bổ sung một mạng Wi-Fi vào danh sách được tin tưởng

Bạn có thể cho phép người dùng kết nối đến các mạng Wi-Fi mà bạn coi là bảo mật, ví dụ như mạng Wi-Fi doanh nghiệp. Để làm điều này, bạn phải thêm mạng vào danh sách các mạng Wi-Fi được tin tưởng. Kiểm soát Thiết bị sẽ chặn truy cập đến tất cả các mạng Wi-Fi ngoài các mạng được quy định trong danh sách được tin tưởng.

Để bổ sung một mạng Wi-Fi vào danh sách được tin tưởng:

1. Mở cửa sổ cấu hình ứng dụng.
2. Ở phần bên trái của cửa sổ, trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát Thiết bị**.
   Ở phần bên phải của cửa sổ, cấu hình của thành phần Kiểm soát Thiết bị sẽ được hiển thị.
3. Ở phần bên phải của cửa sổ, chọn thẻ **Các loại thiết bị**.
   Thẻ **Các loại thiết bị** chứa quy tắc truy cập cho tất cả các thiết bị được bao gồm trong phân loại của thành phần Kiểm soát Thiết bị.
4. Trong cột **Truy cập** đối diện thiết bị **Wi-Fi**, nhấn phải chuột để mở menu ngữ cảnh.
5. Chọn mục **Chặn với ngoại lệ**.
6. Trong danh sách các thiết bị, chọn **Wi-Fi** và nhấn nút **Chỉnh sửa**.
   Việc này sẽ mở ra cửa sổ **Mạng Wi-Fi tin tưởng**.
7. Nhấn vào nút **Thêm**.
   Việc này sẽ mở ra cửa sổ **Mạng Wi-Fi tin tưởng**.
8. Trong cửa sổ **Mạng Wi-Fi tin tưởng**:
   - Trong trường **Tên mạng**, nhập tên của mạng Wi-Fi mà bạn muốn thêm vào danh sách tin tưởng.
   - Trong danh sách thả xuống **Loại xác thực**, chọn kiểu xác thực được sử dụng khi kết nối đến mạng Wi-Fi được tin tưởng.
   - Trong danh sách thả xuống **Loại mã hóa**, chọn kiểu mã hóa được sử dụng để bảo mật lưu lượng của mạng Wi-Fi được tin tưởng.
   - Trong trường **Bình luận**, bạn có thể nhập bất kỳ thông tin nào về mạng Wi-Fi được bổ sung.

   Một mạng Wi-Fi được coi là tin tưởng nếu cấu hình của nó khớp với tất cả các cấu hình được quy định trong quy tắc.
9. Trong cửa sổ **Mạng Wi-Fi tin tưởng**, nhấn **OK**.
10. Trong cửa sổ **Mạng Wi-Fi tin tưởng**, nhấn **OK**.

Sửa một quy tắc truy cập bus kết nối

Để sửa một quy tắc truy cập bus kết nối:

1. Mở cửa sổ cấu hình ứng dụng.

2. Ở phần bên trái của cửa sổ, trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát Thiết bị**.
   Ở phần bên phải của cửa sổ, cấu hình của thành phần Kiểm soát Thiết bị sẽ được hiển thị.

3. Chọn thẻ **Các Bus kết nối**
   Thẻ **Các Bus kết nối** hiển thị quy tắc truy cập cho tất cả các bus kết nối được phân loại trong thành phần Kiểm soát Thiết bị.

4. Chọn quy tắc kết nối bus mà bạn muốn sửa.

5. Thay đổi giá trị của tham số truy cập:

   - Để cho phép truy cập đến một bus kết nối, nhấn vào cột **Truy cập** để mở ra menu ngữ cảnh và chọn **Cho phép**.

   - Để chặn truy cập đến một bus kết nối, nhấn vào cột **Truy cập** để mở ra menu ngữ cảnh và chọn **Ngăn chặn**.

6. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Hành động với các thiết bị được tin tưởng

Mục này chứa thông tin về các hành động với thiết bị được tin tưởng.

Bổ sung một thiết bị vào danh sách Được Tin tưởng từ giao diện ứng dụng

Theo mặc định, khi một thiết bị được thêm vào danh sách các thiết bị được tin tưởng, quyền truy cập thiết bị đó sẽ được cấp cho tất cả người dùng (nhóm người dùng Tất cả mọi người).

Để bổ sung một thiết bị vào danh sách Được Tin tưởng từ giao diện ứng dụng:

1. Mở cửa sổ cấu hình ứng dụng.

2. Ở phần bên trái của cửa sổ, trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát Thiết bị**.
   Ở phần bên phải của cửa sổ, cấu hình của thành phần Kiểm soát Thiết bị sẽ được hiển thị.

3. Ở phần bên phải của cửa sổ, chọn thẻ **Thiết bị được tin tưởng**.

4. Nhấn nút **Lựa chọn**.
   Cửa sổ **Chọn thiết bị được tin tưởng** sẽ được mở ra.

5. Chọn hộp kiểm cạnh tên của thiết bị mà bạn muốn thêm vào danh sách các thiết bị được tin tưởng.
   Danh sách trong cột **Các thiết bị** phụ thuộc vào giá trị được lựa chọn trong danh sách thả xuống **Hiển thị các thiết bị kết nối**.

6. Nhấn nút **Lựa chọn**.
   Cửa sổ **Chọn Người dùng hoặc Nhóm Người dùng** trong Microsoft Windows sẽ được mở ra.

7. Trong cửa sổ **Chọn Người dùng hoặc Nhóm Người dùng** của Microsoft Windows, quy định người dùng và / hoặc nhóm người dùng mà đối với họ, Kaspersky Endpoint Security xác định thiết bị được lựa chọn là đáng tin tưởng.

   Tên của người dùng và / hoặc nhóm người dùng được quy định trong cửa sổ **Chọn người dùng và / hoặc nhóm người dùng** của Microsoft Windows được hiển thị trong trường **Cho phép người dùng và / hoặc nhóm người dùng**.

8. Trong cửa sổ **Chọn thiết bị được tin tưởng**, nhấn **OK**.

   Trong bảng, trên thẻ **Thiết bị được tin tưởng** của cửa sổ cấu hình thành phần **Kiểm soát Thiết bị**, một dòng sẽ xuất hiện và hiển thị tham số của thiết bị được tin tưởng vừa được bổ sung.

9. Lặp lại các bước 4-7 cho mỗi thiết bị mà bạn muốn thêm vào danh sách các thiết bị được tin tưởng cho người dùng và / hoặc nhóm người dùng được quy định.

10. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Bổ sung thiết bị vào danh sách Được Tin tưởng dựa trên mẫu thiết bị hoặc ID thiết bị

Theo mặc định, khi một thiết bị được thêm vào danh sách các thiết bị được tin tưởng, quyền truy cập thiết bị đó sẽ được cấp cho tất cả người dùng (nhóm người dùng Tất cả mọi người).

Để bổ sung thiết bị vào danh sách Được Tin tưởng dựa trên mẫu thiết bị hoặc ID thiết bị:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.

2. Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, mở thư mục với tên của nhóm quản trị mà bạn muốn tạo một danh sách các thiết bị được tin tưởng.

3. Trong không gian làm việc, chọn thẻ **Chính sách**.

4. Chọn chính sách cần thiết.

5. Mở cửa sổ **Thuộc tính: <Tên chính sách>** sử dụng một trong những phương pháp sau đây:

   - Trong menu ngữ cảnh của chính sách, chọn **Thuộc tính**.

   - Nhấn vào liên kết **Thiết lập chính sách** được đặt ở phần bên phải của không gian làm việc của Bảng điều khiển Quản trị.

6. Trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát Thiết bị**.

7. Ở phần bên phải của cửa sổ, chọn thẻ **Thiết bị được tin tưởng**.

8. Nhấn vào nút **Thêm**.

   Menu ngữ cảnh của nút sẽ được mở ra.

9. Trong menu ngữ cảnh của nút **Thêm**, thực hiện một trong các thao tác sau:

   - Chọn nút **Thiết bị bằng ID** nếu bạn muốn chọn các thiết bị có ID riêng đã biết để thêm vào danh sách các thiết bị được tin tưởng.

- Chọn mục **Thiết bị bằng model** để thêm vào danh sách các thiết bị được tin tưởng đã biết VID (ID nhà cung cấp) và PID (ID sản phẩm).

10. Trong cửa sổ được mở ra, trong danh sách thả xuống **Loại thiết bị**, chọn loại thiết bị được hiển thị trong bảng dưới đây.

11. Nhấn vào nút **Làm mới**.

    Bảng này hiển thị một danh sách các thiết bị có ID thiết bị và / hoặc mẫu thiết bị đã biết thuộc loại được chọn trong danh sách thả xuống **Loại thiết bị**.

12. Chọn các hộp kiểm cạnh tên của thiết bị mà bạn muốn thêm vào danh sách các thiết bị được tin tưởng.

13. Nhấn nút **Lựa chọn**.

    Cửa sổ **Chọn Người dùng hoặc Nhóm Người dùng** trong Microsoft Windows sẽ được mở ra.

14. Trong cửa sổ **Chọn Người dùng hoặc Nhóm Người dùng** của Microsoft Windows, quy định người dùng và / hoặc nhóm người dùng mà đối với họ, Kaspersky Endpoint Security xác định thiết bị được lựa chọn là đáng tin tưởng.

    Tên của người dùng và / hoặc nhóm người dùng được quy định trong cửa sổ **Chọn người dùng và / hoặc nhóm người dùng** của Microsoft Windows được hiển thị trong trường **Cho phép người dùng và / hoặc nhóm người dùng**.

15. Nhấn **OK**.

    Các dòng hiển thị với tham số của thiết bị được tin tưởng đã được thêm sẽ xuất hiện trong bảng trên thẻ **Thiết bị được tin tưởng**.

16. Nhấn **OK** hoặc **Áp dụng** để lưu thay đổi.

Bổ sung thiết bị vào danh sách Được Tin tưởng dựa trên mặt nạ của ID thiết bị

Theo mặc định, khi một thiết bị được thêm vào danh sách các thiết bị được tin tưởng, quyền truy cập thiết bị đó sẽ được cấp cho tất cả người dùng (nhóm người dùng Tất cả mọi người).

Thiết bị chỉ có thể được thêm vào danh sách Được Tin tưởng dựa trên mặt nạ ID thiết bị trong Bảng điều khiển Quản trị Kaspersky Security Center.

Để bổ sung thiết bị vào danh sách Được Tin tưởng dựa trên mặt nạ của ID thiết bị:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.

2. Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, mở thư mục với tên của nhóm quản trị mà bạn muốn tạo một danh sách các thiết bị được tin tưởng.

3. Trong không gian làm việc, chọn thẻ **Chính sách**.

4. Chọn chính sách cần thiết.

5. Mở cửa sổ **Thuộc tính: <Tên chính sách>** sử dụng một trong những phương pháp sau đây:

- Trong menu ngữ cảnh của chính sách, chọn **Thuộc tính**.
- Nhấn vào liên kết **Thiết lập chính sách** được đặt ở phần bên phải của không gian làm việc của Bảng điều khiển Quản trị.

6. Trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát Thiết bị**.
7. Ở phần bên phải của cửa sổ, chọn thẻ **Thiết bị được tin tưởng**.
8. Nhấn vào nút **Thêm**.

   Menu ngữ cảnh của nút sẽ được mở ra.
9. Trong menu ngữ cảnh của nút **Thêm**, chọn mục **Thiết bị bằng ID đại diện**.

   Cửa sổ **Thêm thiết bị tin tưởng bằng ID đại diện** sẽ được mở ra.
10. Trong cửa sổ **Thêm thiết bị tin tưởng bằng ID đại diện**, nhập mặt nạ cho các ID thiết bị trong trường **Đại diện**.
11. Nhấn nút **Lựa chọn**.

    Cửa sổ **Chọn Người dùng hoặc Nhóm Người dùng** trong Microsoft Windows sẽ được mở ra.
12. Trong cửa sổ **Chọn Người dùng hoặc Nhóm Người dùng** của Microsoft Windows, quy định người dùng và / hoặc nhóm người dùng mà đối với họ, Kaspersky Endpoint Security xác định thiết bị có mẫu hoặc ID khớp với mặt nạ được quy định là đáng tin tưởng.

    Tên của người dùng và / hoặc nhóm người dùng được quy định trong cửa sổ **Chọn người dùng và / hoặc nhóm người dùng** của Microsoft Windows được hiển thị trong trường **Cho phép người dùng và / hoặc nhóm người dùng**.
13. Nhấn **OK**.

    Trong bảng ở trên thẻ **Thiết bị được tin tưởng** của cửa sổ cấu hình thành phần **Kiểm soát Thiết bị**, một dòng sẽ xuất hiện với cấu hình của quy tắc để thêm các thiết bị vào danh sách thiết bị được tin tưởng theo mặt nạ ID của chúng.
14. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Thiết lập quyền truy cập của người dùng đến một thiết bị được tin tưởng

Theo mặc định, khi một thiết bị được thêm vào danh sách các thiết bị được tin tưởng, quyền truy cập thiết bị đó sẽ được cấp cho tất cả người dùng (nhóm người dùng Tất cả mọi người). Bạn có thể thiết lập quyền truy cập của người dùng (hoặc nhóm người dùng) đến một thiết bị được tin tưởng.

Để thiết lập quyền truy cập của người dùng đến một thiết bị được tin tưởng:

1. Mở cửa sổ cấu hình ứng dụng.
2. Ở phần bên trái của cửa sổ, trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát Thiết bị**.

   Ở phần bên phải của cửa sổ, cấu hình của thành phần Kiểm soát Thiết bị sẽ được hiển thị.
3. Ở phần bên phải của cửa sổ, chọn thẻ **Thiết bị được tin tưởng**.

4. Trong danh sách các thiết bị được tin tưởng, chọn một thiết bị mà bạn muốn sửa quy tắc truy cập.
5. Nhấn nút **Chỉnh sửa**.

   Cửa sổ **Cấu hình quy tắc truy xuất thiết bị tin tưởng** sẽ được mở ra.
6. Nhấn nút **Lựa chọn**.

   Cửa sổ **Chọn Người dùng hoặc Nhóm Người dùng** trong Microsoft Windows sẽ được mở ra.
7. Trong cửa sổ **Chọn Người dùng hoặc Nhóm Người dùng** của Microsoft Windows, quy định người dùng và / hoặc nhóm người dùng mà đối với họ, Kaspersky Endpoint Security xác định thiết bị được lựa chọn là đáng tin tưởng.
8. Nhấn **OK**.

   Tên của người dùng và / hoặc nhóm người dùng được quy định trong cửa sổ **Chọn người dùng và / hoặc nhóm người dùng** của Microsoft Windows được hiển thị trong trường **Cho phép người dùng và / hoặc nhóm người dùng** của cửa sổ **Cấu hình quy tắc truy xuất thiết bị tin tưởng**.
9. Nhấn **OK**.
10. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Xóa thiết bị khỏi danh sách các thiết bị được tin tưởng

Để xóa thiết bị khỏi danh sách các thiết bị được tin tưởng:

1. Mở cửa sổ cấu hình ứng dụng.
2. Ở phần bên trái của cửa sổ, trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát Thiết bị**.

   Ở phần bên phải của cửa sổ, cấu hình của thành phần Kiểm soát Thiết bị sẽ được hiển thị.
3. Ở phần bên phải của cửa sổ, chọn thẻ **Thiết bị được tin tưởng**.
4. Chọn thiết bị mà bạn muốn xóa khỏi danh sách các thiết bị được tin tưởng.
5. Nhấn nút **Gỡ bỏ**.
6. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Một quyết định truy cập đến một thiết bị mà bạn đã xóa khỏi danh sách các thiết bị tin tưởng được thực hiện bởi Kaspersky Endpoint Security dựa trên các quy tắc truy cập thiết bị và quy tắc truy cập bus kết nối.

Sửa mẫu thông điệp Kiểm soát Thiết bị

Khi người dùng cố gắng truy cập một thiết bị bị chặn, Kaspersky Endpoint Security sẽ hiển thị một thông điệp cho biết việc truy cập thiết bị đã bị chặn, hoặc một hoạt động với nội dung của thiết bị đã bị ngăn cấm. Nếu người dùng tin rằng việc truy cập đến thiết bị đã bị chặn nhầm hoặc một hoạt động với nội dung thiết bị đã bị cấm nhầm, người dùng có thể sử dụng gửi một thông điệp đến quản trị viên mạng doanh nghiệp cục bộ bằng cách nhấn vào liên kết trong thông điệp được hiển thị về hành động bị chặn.

Các mẫu có thể được sử dụng cho các thông điệp về việc chặn truy cập đến thiết bị hoặc cấm hoạt động với nội dung thiết bị, và cho các thông điệp được gửi đến quản trị viên. Bạn có thể sửa mẫu thông điệp.

Để sửa các mẫu thông điệp cho Kiểm soát Thiết bị:

1. Mở cửa sổ cấu hình ứng dụng.
2. Ở phần bên trái của cửa sổ, trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát Thiết bị**.
   Ở phần bên phải của cửa sổ, cấu hình của thành phần Kiểm soát Thiết bị sẽ được hiển thị.
3. Ở phía bên phải của cửa sổ, bấm vào nút **Mẫu**.
   Cửa sổ **Tin nhắn mẫu** sẽ được mở ra.
4. Thực hiện một trong các thao tác sau:
   - Để sửa mẫu của thông điệp về việc chặn truy cập đến một thiết bị hoặc cấm hoạt động với nội dung của thiết bị, chọn thẻ **Thông báo**.
   - Để sửa mẫu thông điệp được gửi đến quản trị viên mạng LAN, chọn thẻ **Thông điệp đến quản trị viên**.
5. Sửa mẫu thông điệp. Bạn cũng có thể sử dụng các nút sau: **Biến số**, **Mặc định**, và **Liên kết** (nút này chỉ có thể được sử dụng trên thẻ **Thông báo**).
6. Nhấn **OK**.
7. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Nhận truy cập đến một thiết bị bị chặn

Các chỉ dẫn này dành cho người sử dụng của máy khách có cài đặt Kaspersky Endpoint Security.

Chức năng của Kaspersky Endpoint Security cấp quyền truy cập tạm thời đến một thiết bị chỉ khả dụng khi Kaspersky Endpoint Security hoạt động theo chính sách của Kaspersky Security Center và chức năng này được bật trong cấu hình chính sách (xem *Hướng dẫn dành cho Quản trị viên Kaspersky Security Center*).

Để yêu cầu truy cập đến một thiết bị bị chặn từ cửa sổ cấu hình thành phần Kiểm soát Thiết bị:

1. Trong cửa sổ chính của ứng dụng, chọn thẻ **Bảo vệ và Kiểm soát**.
2. Nhấn vào mục **Bảng kiểm soát**.
   Mục **Bảng kiểm soát** sẽ được mở ra.
3. Nhấn phải chuột để gọi menu ngữ cảnh của dòng có chứa thông tin về thành phần Kiểm soát Thiết bị.
   Một menu để chọn hành động đối với thành phần sẽ được mở ra.
4. Nhấn nút **Truy xuất đến thiết bị**.
   Cửa sổ **Yêu cầu truy xuất đến thiết bị** sẽ được mở ra.
5. Từ danh sách các thiết bị được kết nối, chọn thiết bị mà bạn muốn truy cập.

6. Nhấn nút **Tạo tập tin yêu cầu truy cập**.

   Việc này sẽ mở ra cửa sổ **Tạo tập tin yêu cầu truy cập**.

7. Trong trường **Truy cập trong khi thực thi**, quy định khoảng thời gian mà bạn muốn truy cập đến thiết bị.

8. Nhấp vào nút **Lưu**.

   Điều này sẽ mở ra cửa sổ **Lưu tập tin yêu cầu truy cập** tiêu chuẩn trong Microsoft Windows.

9. Trong cửa sổ **Lưu tập tin yêu cầu truy cập** của Microsoft Windows, chọn thư mục mà bạn muốn lưu tập tin yêu cầu truy cập cho thiết bị, và nhấn nút **Lưu**.

10. Gửi tập tin yêu cầu truy cập vào thiết bị đến quản trị viên mạng LAN.

11. Nhận tập tin khóa truy cập thiết bị từ quản trị viên mạng LAN.

12. Trong cửa sổ **Yêu cầu truy xuất đến thiết bị**, nhấn nút **Kích hoạt khóa truy cập**.

    Cửa sổ **Mở khóa truy xuất** tiêu chuẩn trong Microsoft Windows sẽ được mở ra.

13. Trong cửa sổ **Mở khóa truy xuất** của Microsoft Windows, chọn tập tin khóa truy cập thiết bị mà bạn được nhận từ quản trị viên mạng LAN và nhấn **Mở**.

    Cửa sổ **Kích hoạt khóa truy cập cho thiết bị** sẽ được mở ra và hiển thị thông tin về quyền truy cập được cấp.

14. Trong cửa sổ **Kích hoạt khóa truy cập cho thiết bị**, nhấn **OK**.

Để yêu cầu truy cập đến một thiết bị bị chặn thông qua liên kết trong thông điệp báo thiết bị đã bị chặn:

1. Trong cửa sổ với thông điệp báo rằng thiết bị hoặc bus kết nối đã bị chặn, nhấn liên kết **Yêu cầu truy cập**.

   Việc này sẽ mở ra cửa sổ **Tạo tập tin yêu cầu truy cập**.

2. Trong trường **Truy cập trong khi thực thi**, quy định khoảng thời gian mà bạn muốn truy cập đến thiết bị.

3. Nhấp vào nút **Lưu**.

   Điều này sẽ mở ra cửa sổ **Lưu tập tin yêu cầu truy cập** tiêu chuẩn trong Microsoft Windows.

4. Trong cửa sổ **Lưu tập tin yêu cầu truy cập** của Microsoft Windows, chọn thư mục mà bạn muốn lưu tập tin yêu cầu truy cập cho thiết bị, và nhấn nút **Lưu**.

5. Gửi tập tin yêu cầu truy cập vào thiết bị đến quản trị viên mạng LAN.

6. Nhận tập tin khóa truy cập thiết bị từ quản trị viên mạng LAN.

7. Trong cửa sổ **Yêu cầu truy xuất đến thiết bị**, nhấn nút **Kích hoạt khóa truy cập**.

   Cửa sổ **Mở khóa truy xuất** tiêu chuẩn trong Microsoft Windows sẽ được mở ra.

8. Trong cửa sổ **Mở khóa truy xuất** của Microsoft Windows, chọn tập tin khóa truy cập thiết bị mà bạn được nhận từ quản trị viên mạng LAN và nhấn **Mở**.

   Cửa sổ **Kích hoạt khóa truy cập cho thiết bị** sẽ được mở ra và hiển thị thông tin về quyền truy cập được cấp.

9. Trong cửa sổ **Kích hoạt khóa truy cập cho thiết bị**, nhấn **OK**.

Khoảng thời gian được cấp quyền truy cập đến thiết bị có thể khác với lượng thời gian mà bạn đã yêu cầu. Quyền truy cập đến thiết bị sẽ được cấp cho khoảng thời gian mà quản trị viên mạng máy tính cục bộ quy định khi tạo khóa truy cập đến thiết bị.

Tạo khóa để truy cập một thiết bị bị chặn sử dụng Kaspersky Security Center

Để cấp quyền truy cập tạm thời cho người dùng đến một thiết bị bị chặn, một khóa truy cập đến thiết bị là cần thiết. Bạn có thể tạo một khóa truy cập sử dụng Kaspersky Security Center.

Để tạo một khóa truy cập cho một thiết bị bị chặn:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, mở thư mục với tên của nhóm quản trị chứa máy khách liên quan.
3. Trong không gian làm việc, chọn thẻ **Các thiết bị**.
4. Trong danh sách máy khách, chọn máy tính mà người dùng trên đó muốn được cấp quyền truy cập tạm thời đến một thiết bị bị khóa.
5. Trong menu ngữ cảnh của máy tính, chọn **Cấp quyền truy cập vào thiết bị và các dữ liệu ở chế độ ngoại tuyến**.

   Cửa sổ **Cấp quyền truy cập vào thiết bị và các dữ liệu ở chế độ ngoại tuyến** sẽ được mở ra.
6. Chọn thẻ **Kiểm soát Thiết bị**.
7. Trên thẻ **Kiểm soát Thiết bị**, nhấn nút **Duyệt**.

   Cửa sổ **Lựa chọn tập tin yêu cầu truy cập** tiêu chuẩn của Microsoft Windows sẽ được mở ra.
8. Trong cửa sổ **Lựa chọn tập tin yêu cầu truy cập**, chọn tập tin yêu cầu truy cập mà bạn được nhận từ người dùng và nhấn nút **Mở**.

   Kiểm soát Thiết bị sẽ hiển thị thông tin của thiết bị bị khóa cho người dùng đã yêu cầu truy cập.
9. Quy định giá trị của cấu hình **Thời hạn truy cập**.

   Cấu hình này quy định thời lượng truy cập đến thiết bị bị khóa được cấp cho người dùng. Giá trị mặc định là giá trị được quy định bởi người dùng khi họ tạo ra tập tin yêu cầu truy cập.
10. Quy định giá trị của cấu hình **Thời gian kích hoạt**

    Cấu hình này quy định khoảng thời gian mà trong đó người dùng có thể kích hoạt việc truy cập đến thiết bị bị chặn bằng cách sử dụng khóa truy cập.
11. Nhấp vào nút **Lưu**.

    Điều này sẽ mở ra cửa sổ **Lưu khóa truy cập** tiêu chuẩn trong Microsoft Windows.
12. Chọn thư mục đích mà bạn muốn lưu tập tin chứa khóa truy cập vào thiết bị bị chặn.
13. Nhấp vào nút **Lưu**.

Kiểm soát web

Thành phần này có thể được sử dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Microsoft Windows cho máy trạm. Thành phần này không thể được sử dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Microsoft Windows cho máy chủ tập tin.

Mục này chứa thông tin về Kiểm soát web và chỉ dẫn cách để thiết lập cấu hình thành phần.

Thông tin về Kiểm soát web

Kiểm soát web cho phép kiểm soát hành động bởi người dùng LAN bằng cách hạn chế hoặc chặn quyền truy cập đến các tài nguyên web.

Một tài nguyên web là một trang web riêng lẻ hoặc nhiều trang web, hay một website hoặc nhiều website có một đặc điểm chung.

Kiểm soát web cung cấp các tùy chọn sau:

- Tiết kiệm lưu lượng.

  Lưu lượng được kiểm soát bằng cách hạn chế hoặc chặn việc tải về các tập tin đa phương tiện, hoặc bằng cách hạn chế hoặc chặn việc truy cập đến các tài nguyên web không liên quan đến trách nhiệm công việc của người dùng.

- Bỏ giới hạn truy cập theo hạng mục nội dung của tài nguyên web.

  Để tiết kiệm lưu lượng và giảm thiểu tổn thất tiềm năng từ việc sử dụng sai thời gian của nhân viên, bạn có thể hạn chế hoặc chặn truy cập đến các hạng mục tài nguyên web cụ thể (ví dụ, chặn truy cập đến các tài nguyên web thuộc hạng mục "Phương tiện truyền thông Internet").

- Kiểm soát tập trung truy cập đến các tài nguyên web.

  Khi sử dụng Kaspersky Security Center, bạn có thể cấu hình truy cập đến tài nguyên web theo cá nhân và nhóm.

Tất cả các quy định hạn chế và chặn được áp dụng cho việc truy cập đến tài nguyên web đều được triển khai dưới dạng quy tắc truy cập tài nguyên web.

Bật và tắt Kiểm soát web

Theo mặc định, Kiểm soát web sẽ được bật. Bạn có thể tắt Kiểm soát web nếu cần thiết.

Có hai cách để bật hoặc tắt thành phần này:

- Trên thẻ **Bảo vệ và Kiểm soát** của cửa sổ chính của ứng dụng
- Từ cửa sổ cấu hình ứng dụng.

*Để bật hoặc tắt Kiểm soát web trên thẻ **Bảo vệ và Kiểm soát** của cửa sổ chính của ứng dụng:*

1. Mở cửa sổ chính của ứng dụng.
2. Chọn thẻ **Bảo vệ và Kiểm soát**.
3. Nhấn vào mục **Bảng kiểm soát**.
   Mục **Bảng kiểm soát** sẽ được mở ra.
4. Nhấn phải chuột để gọi menu ngữ cảnh của dòng có chứa thông tin về thành phần Kiểm soát web.
   Một menu để chọn hành động đối với thành phần sẽ được mở ra.
5. Thực hiện một trong các thao tác sau:
   - Để bật Kiểm soát web, chọn **Bắt đầu** trong menu.
   - Để tắt Kiểm soát web, chọn **Dừng** trong menu.

Để bật hoặc tắt Kiểm soát web từ cửa sổ cấu hình ứng dụng:

1. Mở cửa sổ cấu hình ứng dụng.
2. Ở phần bên trái của cửa sổ, trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát web**.
   Ở phần bên phải của cửa sổ, cấu hình của thành phần Kiểm soát web sẽ được hiển thị.
3. Thực hiện một trong các thao tác sau:
   - Nếu bạn muốn bật Kiểm soát web, chọn hộp kiểm **Bật Kiểm soát web**.
   - Nếu bạn muốn tắt Kiểm soát web, xóa hộp kiểm **Bật Kiểm soát web**.

   Nếu Kiểm soát web bị tắt, Kaspersky Endpoint Security sẽ không kiểm soát việc truy cập đến các tài nguyên web.
4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Hạng mục nội dung của tài nguyên web

Các hạng mục nội dung tài nguyên web (sau đây cũng được gọi là "hạng mục") được liệt kê dưới đây đã được chọn để mô tả đầy đủ nhất các khối dữ liệu được đặt trên tài nguyên web, xét đến các chức năng và tính năng chủ đề của chúng. Thứ tự các hạng mục xuất hiện trong danh sách này không phản ánh tầm quan trọng hay ưu tiên tương đối của chúng trên Internet. Tên của các hạng mục đều là tạm thời và chỉ được sử dụng cho các sản phẩm và website Kaspersky. Tên này không phản ánh ý nghĩa ngầm định của luật pháp. Một tài nguyên web có thể thuộc một vài hạng mục cùng lúc.

Nội dung người lớn

Hạng mục này bao gồm các loại tài nguyên web sau đây:

- Tài nguyên web chứa bất kỳ ảnh hoặc video nào thể hiện bộ phận sinh dục của người hoặc sinh vật giống người, các hành động quan hệ tình dục hoặc tự kích thích tình dục được thực hiện bởi người hoặc các sinh vật giống người.

- Tài nguyên web chứa bất kỳ tài liệu văn bản nào, bao gồm tài liệu văn chương hay nghệ thuật, mô tả bộ phận sinh dục của người hoặc sinh vật giống người, các hành động quan hệ tình dục hoặc tự kích thích tình dục được thực hiện bởi người hoặc các sinh vật giống người.

- Các tài nguyên web chuyên dành cho việc thảo luận về các khía cạnh tình dục của mối quan hệ giữa người với người.

  > Trùng với hạng mục "Phương tiện truyền thông Internet".

- Các tài nguyên web mô tả tài liệu khiêu dâm, các tác phẩm mô tả thực tế hành vi tình dục của người, hoặc các tác phẩm nghệ thuật được thiết kế để kích thích ham muốn tình dục.

- Các tài nguyên web của các kênh truyền thông chính thức và cộng đồng trực tuyến có cơ sở độc giả rõ ràng, chứa một mục chuyên biệt và / hoặc các bài viết cá nhân dành riêng cho khía cạnh tình dục của mối quan hệ giữa người với người.

- Các tài nguyên web dành riêng cho sự lệch lạc tình dục.

- Các tài nguyên web quảng cáo và bán dụng cụ để sử dụng trong tình dục và kích thích ham muốn tình dục, các dịch vụ tình dục và hẹn hò tình dục, bao gồm các dịch vụ được cung cấp trực tuyến thông qua tán gẫu khiêu dâm video, "tình dục qua điện thoại", "nhắn tin khiêu dâm" ("tình dục ảo").

- Các tài nguyên web với nội dung sau:

  - Các bài viết và blog bàn về giáo dục giới tính với cả chủ đề khoa học lẫn phổ biến.

  - Các bách khoa toàn thư y tế, cụ thể các phần về sinh sản tình dục.

  - Tài nguyên của các tổ chức y tế, cụ thể là các phần về điều trị bộ phận sinh dục.

Phần mềm, âm thanh, video

Hạng mục này chứa các hạng mục con sau đây mà bạn có thể lựa chọn:

- **Âm thanh và video**.

  Hạng mục con này bao gồm các tài nguyên web phân bổ tài liệu âm thanh và video: phim ảnh, bản ghi truyền hình thể thao, nhật ký các buổi giao hưởng, bài hát, đoạn phim, video, nhật ký âm thanh và video giáo dục, v.v...

- **Torrent**.

  Hạng mục con này bao gồm các website torrent tracker được sử dụng để chia sẻ các tập tin có kích cỡ không giới hạn.

- **Chia sẻ tập tin**.

  Hạng mục con này bao gồm các website chia sẻ tập tin bất kể vị trí địa lý của tập tin đang được phân phối.

Rượu, thuốc lá và chất gây nghiện

Hạng mục này bao gồm các tài nguyên web có nội dung liên quan trực tiếp hoặc gián tiếp đến các sản phẩm rượu bia hoặc có cồn, các sản phẩm thuốc lá, chất gây nghiện, chất gây ảo giác và / hoặc chất làm say.

- Các tài nguyên web quảng cáo và bán các chất đó cũng như các vật dụng để sử dụng chúng.

  Trùng với hạng mục "Thương mại điện tử".

- Các tài nguyên web kèm chỉ dẫn về việc sử dụng hoặc sản xuất các chất gây nghiện, chất gây ảo giác và / hoặc chất làm say.

Hạng mục này bao gồm các tài nguyên web đề cập đến các chủ đề khoa học và y tế.

Bạo lực

Hạng mục này bao gồm các tài nguyên web có chứa bất kỳ hình ảnh, video hoặc văn bản tài liệu nào mô tả các hành vi bạo lực thể xác hay tinh thần chống lại con người, hoặc đối xử tàn nhẫn với động vật.

- Các tài nguyên web thể hiện hoặc mô tả hình ảnh các vụ hành quyết, tra tấn, hoặc lạm dụng, cũng như các công cụ dùng cho các hành vi đó.

  Trùng với hạng mục "Vũ khí, chất nổ, chất phóng hỏa".

- Các tài nguyên web thể hiện hoặc mô tả hình ảnh giết người, đánh nhau, hành hung, hoặc hiếp dâm, các hình ảnh trong đó con người, động vật, hoặc sinh vật tưởng tượng đang bị lạm dụng hoặc lăng nhục.

- Các tài nguyên web với những thông tin kích động hành vi gây nguy hiểm cho cuộc sống và / hoặc sức khỏe, bao gồm cả tự hại bản thân hoặc tự sát.

- Tài nguyên web với những thông tin chứng minh hay biện hộ việc chấp nhận bạo lực và / hoặc sự tàn ác, hoặc kích động hành vi bạo lực chống lại con người hoặc động vật.

- Các tài nguyên Web thể hiện cụ thể hiện thực hoặc mô tả các nạn nhân và sự tàn bạo của chiến tranh, xung đột vũ trang, và các cuộc đụng độ quân sự, tai nạn, thảm họa, thiên tai, biến động xã hội hoặc công nghiệp, hay nỗi khổ đau của con người.

- Những trò chơi trên trình duyệt máy tính với cảnh quay bạo lực và tàn ác, bao gồm các trò "bắn súng", "chiến đấu", "chém giết", v.v...

  Trùng với hạng mục "Trò chơi máy tính".

Vũ khí, chất nổ, chất phóng hỏa

Hạng mục này bao gồm các tài nguyên web với thông tin về các loại vũ khí, chất nổ và chất phóng hỏa:

- Website của các nhà sản xuất và cửa hàng bán vũ khí, chất nổ và chất phóng hỏa.

  Trùng với hạng mục "Thương mại điện tử".

- Các tài nguyên web dành riêng cho việc sản xuất hoặc sử dụng vũ khí, chất nổ và chất phóng hỏa.
- Các tài nguyên web chứa các tài liệu về phân tích, lịch sử, chế tạo, và các tài liệu bách khoa toàn thư riêng dành cho vũ khí, chất nổ, và chất phóng hỏa.

Thuật ngữ "vũ khí" có nghĩa là các thiết bị, vật phẩm, phương tiện được thiết kế nhằm gây hại cho cuộc sống và sức khoẻ của con người và động vật và / hoặc làm hư hỏng thiết bị và nhà cửa.

Tục tĩu

Hạng mục này bao gồm các tài nguyên web có ngôn ngữ tục tĩu đã được phát hiện.

Trùng với hạng mục "Nội dung người lớn".

Hạng mục này cũng bao gồm các tài nguyên web với tài liệu ngôn ngữ và ngữ văn chứa nội dung tục tĩu là chủ đề được nghiên cứu.

Cờ bạc, xổ số, rút thăm trúng thưởng

Hạng mục này bao gồm các tài nguyên web mời chào người dùng tham gia đánh bạc, kể cả nếu việc tham gia như vậy không phải là một điều kiện bắt buộc để truy cập vào website. Hạng mục này bao gồm các tài nguyên web cung cấp:

- Đánh bạc, trong đó những người tham gia bắt buộc phải đóng góp tiền.

  Trùng với hạng mục "Trò chơi máy tính".

- Rút thăm trúng thưởng liên quan đến cá cược bằng tiền.
- Xổ số liên quan đến việc mua vé hoặc số.
- Thông tin có thể gây ra việc mong muốn tham gia vào đánh bạc, rút thăm trúng thưởng, và xổ số.

Trùng với hạng mục "Thương mại điện tử".

Hạng mục này bao gồm các trò chơi cho phép tham gia chơi miễn phí trong một chế độ riêng biệt, cũng như các tài nguyên web tích cực quảng cáo các tài nguyên web thuộc hạng mục này đến người dùng.

Truyền thông Mạng

Hạng mục này bao gồm các tài nguyên web cho phép người sử dụng (dù đã đăng ký hay chưa) gửi tin nhắn cá nhân cho người dùng khác của các tài nguyên web có liên quan hoặc các dịch vụ trực tuyến khác và / hoặc thêm nội dung (dù mở hay đóng đến công chúng) vào các tài nguyên web có các từ khóa nhất định. Bạn có thể chọn riêng những hạng mục con sau đây:

- **Tán gẫu và diễn đàn**.

  Những hạng mục con này bao gồm những tài nguyên web dành cho thảo luận công khai về nhiều chủ đề sử dụng các ứng dụng web đặc biệt, cũng như các tài nguyên web được thiết kế để phân phối hoặc hỗ trợ các ứng dụng nhắn tin tức thời cho phép giao tiếp thời gian thực.

- **Blog**.

  Những hạng mục con này bao gồm các nền tảng blog, là những website cung cấp những dịch vụ có trả tiền hoặc miễn phí cho việc tạo lập và duy trì blog.

- **Mạng xã hội**.

  Hạng mục con này bao gồm các website được thiết kế để xây dựng, hiển thị và quản lý địa chỉ liên lạc giữa các cá nhân, tổ chức, và các chính phủ, trong đó việc đăng ký một tài khoản người dùng là một điều kiện để tham gia.

- **Trang web hẹn hò**.

  Hạng mục con này bao gồm những tài nguyên web đóng vai trò như một mô hình mạng xã hội cung cấp dịch vụ có trả tiền hoặc miễn phí.

  > Trùng với các hạng mục "Nội dung người lớn" và "Thương mại điện tử".

- **Email trên web**.

  Hạng mục con này bao gồm các trang đăng nhập riêng vào một dịch vụ email và các hộp thư có chứa các email và các dữ liệu liên quan (như danh bạ cá nhân). Hạng mục này không bao gồm các trang web khác của một nhà cung cấp dịch vụ Internet cũng cung cấp dịch vụ email.

Các hệ thống bán lẻ điện tử, ngân hàng và thanh toán

Hạng mục này bao gồm những các tài nguyên web được thiết kế cho bất kỳ giao dịch trực tuyến không sử dụng tiền mặt nào, sử dụng các ứng dụng web có mục đích chuyên biệt. Bạn có thể chọn riêng những hạng mục con sau đây:

- **Cửa hàng và đấu giá**.

  Hạng mục con này bao gồm các cửa hàng trực tuyến và các trang đấu giá bán bất kỳ hàng hóa, công trình hoặc dịch vụ nào cho các cá nhân và / hoặc pháp nhân, bao gồm cả website của các cửa hàng tiến hành bán hàng độc quyền trực tuyến và hồ sơ trực tuyến của các cửa hàng bán lẻ có gian hàng chấp nhận thanh toán trực tuyến.

- **Ngân hàng**.

  Hạng mục con này bao gồm các trang web chuyên biệt của các ngân hàng với chức năng ngân hàng trực tuyến, bao gồm điện chuyển tiền (điện tử) chuyển giữa các tài khoản ngân hàng, nộp tiền vào ngân hàng, thực hiện chuyển đổi ngoại hối, chi trả cho các dịch vụ của bên thứ ba, v.v...

- **Hệ thống thanh toán**.

  Hạng mục con này bao gồm các trang web của hệ thống tiền điện tử cung cấp quyền truy cập vào tài khoản cá nhân của người dùng.

Theo thuật ngữ kỹ thuật, thanh toán có thể được thực hiện bằng cách sử dụng bất kỳ loại thẻ ngân hàng (nhựa hoặc ảo, thẻ ghi nợ hoặc thẻ tín dụng, địa phương hay quốc tế) và tiền điện tử nào. Các tài nguyên web có thể rơi vào thể loại này cho dù có hoặc không có các khía cạnh kỹ thuật như truyền tải dữ liệu qua giao thức SSL, việc sử dụng xác thực 3D Secure, v.v...

Tìm kiếm việc làm

Hạng mục này bao gồm các tài nguyên web được thiết kế nhằm quy tụ nhà tuyển dụng và người tìm việc:

- Website của các cơ quan tuyển dụng (cơ quan sử dụng lao động và / hoặc cơ quan săn đầu người).
- Website of người sử dụng lao động với mô tả các vị trí đang tuyển dụng và lợi thế của họ.
- Các cổng thông tin độc lập với đề nghị tuyển dụng từ các nhà sử dụng lao động và cơ quan tuyển dụng.
- Các mạng xã hội chuyên nghiệp giúp đăng tải hoặc tìm kiếm thông tin về các chuyên gia đang không chủ động tìm kiếm việc làm, cùng các chức năng khác.

> Trùng với hạng mục "Phương tiện truyền thông Internet".

Hệ thống truy cập ẩn danh

Hạng mục này bao gồm các tài nguyên web có chức năng trung gian trong việc tải về nội dung của các tài nguyên web khác sử dụng các ứng dụng web đặc biệt vì mục đích:

- Vượt qua hạn chế được áp đặt bởi quản trị viên mạng LAN khi truy cập đến các địa chỉ web hoặc địa chỉ IP;
- Truy cập ẩn danh các tài nguyên web, bao gồm các tài nguyên web từ chối cụ thể những yêu cầu HTTP từ các địa chỉ IP hoặc nhóm địa chỉ IP nhất định (ví dụ, các địa chỉ IP được nhóm chung bởi quốc gia xuất phát).

Hạng mục này cũng bao gồm các tài nguyên web dành riêng cho mục đích được nói ở trên ("ẩn danh") và các tài nguyên web có chức năng tương đương về mặt kỹ thuật.

Trò chơi điện tử

Hạng mục này bao gồm các tài nguyên web dành cho các trò chơi điện tử thuộc nhiều thể loại:

- Website của các nhà phát triển trò chơi điện tử.
- Các tài nguyên web chuyên dành cho việc thảo luận về các trò chơi điện tử.

> Trùng với hạng mục "Phương tiện truyền thông Internet".

- Các tài nguyên web cung cấp khả năng tham gia trực tuyến vào các trò chơi, cùng với những người hoặc cá nhân tham gia khác, với việc cài đặt ứng dụng trên máy tính cục bộ hoặc không cần cài đặt ("game trình duyệt").
- Các tài nguyên web được thiết kế để quảng cáo, phân phối và hỗ trợ phần mềm chơi game.

> Trùng với hạng mục "Thương mại điện tử".

Tôn giáo, liên quan đến tôn giáo

Hạng mục này bao gồm các tài nguyên web với tài liệu về phong trào công khai, các hiệp hội và tổ chức với ý tưởng tôn giáo và / hoặc các giáo phái thuộc đủ mọi thể loại.

- Các website của các tổ chức tôn giáo chính thức thuộc mọi cấp bậc, từ các cộng đồng tôn giáo quốc tế đến địa phương.
- Website của những hiệp hội và cộng đồng tôn giáo không được đăng ký thường xuất hiện do tách khỏi một hiệp hội hoặc cộng đồng tôn giáo lớn.
- Các website của những hiệp hội và cộng đồng tôn giáo xuất hiện độc lập với những phong trào tôn giáo truyền thống, bao gồm theo phát kiến của một nhà sáng lập cụ thể.
- Website của các tổ chức liên nhà thờ theo đuổi sự hợp tác giữa đại diện của những tôn giáo truyền thống khác nhau.
- Các tài nguyên web có nội dung học thuật, lịch sử và bách khoa toàn thư về chủ đề tôn giáo.
- Các tài nguyên web với mô tả hoặc thể hiện chi tiết hành động thờ cúng của giáo phái tôn giáo, bao gồm các nghi thức và lễ nghi liên quan đến việc thờ phụng Chúa Trời, thần linh và / hoặc vật thánh được cho là có sức mạnh siêu nhiên.

Truyền thông

Hạng mục này bao gồm các tài nguyên web với nội dung tin tức công khai được tạo bởi các đơn vị truyền thông đại chúng hoặc đơn vị phát hành trực tuyến cho phép người dùng bổ sung báo cáo tin tức của riêng mình:

- Website của các đơn vị truyền thông chính thức.
- Website cung cấp dịch vụ thông tin có thẩm quyền của những nguồn thông tin chính thức.
- Website cung cấp các dịch vụ tổng hợp thông tin tin tức từ nhiều nguồn chính thức và phi chính thức.
- Website ở đó nội dung tin tức được tạo bởi chính người dùng ("website tin tức xã hội").

> Trùng với hạng mục "Phương tiện truyền thông Internet".

Bảng quảng cáo

Hạng mục này bao gồm các tài nguyên web có bảng quảng cáo. Thông tin quảng cáo trên bảng quảng cáo có thể làm người dùng xao nhãng với hoạt động của họ, việc tải về bảng quảng cáo cũng làm tăng lưu lượng dữ liệu.

Thông tin về quy tắc truy cập tài nguyên web

Một quy tắc truy cập tài nguyên web là một tập hợp các bộ lọc và hành động được Kaspersky Endpoint Security thực hiện khi người dùng truy cập các tài nguyên web được mô tả bởi quy tắc trong khoảng thời gian được quy định trong lịch quy tắc. Bộ lọc cho phép bạn quy định chính xác một nhóm tài nguyên web mà việc truy cập đến đó được kiểm soát bởi thành phần Kiểm soát web.

Các bộ lọc sau có thể được sử dụng:

- **Lọc theo nội dung**. Kiểm soát web sẽ phân loại tài nguyên web theo nội dung và kiểu dữ liệu. Bạn có thể kiểm soát quyền truy cập của người dùng đến các tài nguyên web có nội dung và kiểu dữ liệu thuộc một hạng mục nhất định. Khi người dùng truy cập các tài nguyên web thuộc một hạng mục nội dung và / hoặc hạng mục kiểu dữ liệu được chọn, Kaspersky Endpoint Security sẽ thực hiện hành động được quy định trong quy tắc.

- **Lọc theo địa chỉ tài nguyên web**. Bạn có thể kiểm soát quyền truy cập của người dùng đến tất cả các địa chỉ tài nguyên web hoặc đến các địa chỉ tài nguyên web riêng lẻ và / hoặc nhóm địa chỉ tài nguyên web.

  Nếu bộ lọc theo nội dung và bộ lọc theo địa chỉ tài nguyên web được quy định, và địa chỉ tài nguyên web và / hoặc nhóm địa chỉ tài nguyên web được quy định đó thuộc các hạng mục nội dung hoặc hạng mục kiểu dữ liệu được chọn, Kaspersky Endpoint Security sẽ không kiểm soát quyền truy cập đến tất cả các tài nguyên web trong hạng mục nội dung và / hoặc hạng mục kiểu dữ liệu được chọn. Thay vào đó, ứng dụng sẽ chỉ kiểm soát quyền truy cập đến địa chỉ tài nguyên web và / hoặc nhóm địa chỉ tài nguyên web được quy định.

- **Lọc theo tên của người dùng và nhóm người dùng**. Bạn có thể quy định tên của người dùng và / hoặc nhóm người dùng có quyền truy cập đến tài nguyên web được kiểm soát theo quy tắc.

- **Lịch quy tắc**. Bạn có thể quy định lịch quy tắc. Lịch quy tắc xác định khoảng thời gian mà trong đó Kaspersky Endpoint Security sẽ giám sát việc truy cập đến các tài nguyên web được bao gồm trong quy tắc.

Sau khi Kaspersky Endpoint Security được cài đặt, danh sách quy tắc của thành phần Kiểm soát web sẽ không còn trống. Có hai quy tắc được cài đặt sẵn:

- Quy tắc Tình huống và Bảng Phong cách, cho phép tất cả người dùng truy cập các tài nguyên web có địa chỉ chứa các tập tin với phần mở rộng css, js hoặc vbs bất cứ lúc nào. Ví dụ: http://www.example.com/style.css, http://www.example.com/style.css?mode=normal.

- "Quy tắc mặc định" cho phép tất cả người dùng truy cập đến bất kỳ tài nguyên web vào bất cứ lúc nào.

Hành động với quy tắc truy cập tài nguyên web

Bạn có thể thực hiện các hành động sau trên quy tắc truy cập tài nguyên web:

- Thêm một quy tắc mới

- Sửa một quy tắc

- Gán ưu tiên cho một quy tắc

  Mức độ ưu tiên của một quy tắc được quy định bởi vị trí của dòng chứa mô tả ngắn gọn về quy tắc này trong bảng quy tắc truy cập trong cửa sổ cấu hình của thành phần Kiểm soát web. Điều này có nghĩa một quy tắc ở vị trí cao hơn trong bảng quy tắc truy cập có mức ưu tiên cao hơn quy tắc ở dưới nó.

  Nếu tài nguyên web mà người dùng cố gắng truy cập khớp với tham số của một vài quy tắc, Kaspersky Endpoint Security sẽ thực thi hành động tương ứng với quy tắc có mức độ ưu tiên cao nhất.

- Kiểm tra một quy tắc.

  Bạn có thể kiểm tra sự nhất quán của các quy tắc bằng cách sử dụng chức năng Chẩn đoán Quy tắc.

- Bật và tắt một quy tắc.

  Một quy tắc truy cập tài nguyên web có thể được bật (trạng thái hoạt động: *Bật*) hoặc tắt (trạng thái hoạt động: *Tắt*). Theo mặc định, sau khi một quy tắc được tạo, nó sẽ được bật (trạng thái hoạt động: *Bật*). Bạn có thể tắt một quy tắc.

- Xóa quy tắc

Bổ sung và sửa một quy tắc truy cập tài nguyên web

Để bổ sung hoặc sửa một quy tắc truy cập tài nguyên web

1. Mở cửa sổ cấu hình ứng dụng.
2. Ở phần bên trái của cửa sổ, trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát web**.

   Ở phần bên phải của cửa sổ, cấu hình của thành phần Kiểm soát web sẽ được hiển thị.
3. Thực hiện một trong các thao tác sau:

   - Để bổ sung một quy tắc, nhấn vào nút **Thêm**.
   - Nếu bạn muốn sửa một quy tắc, chọn quy tắc đó trong bảng và nhấn nút **Chỉnh sửa**.

   Cửa sổ **Quy tắc truy cập tài nguyên web** sẽ được mở ra.
4. Nhập hoặc sửa cấu hình của quy tắc. Để làm điều này:

   a. Trong trường **Tên**, nhập hoặc sửa tên của quy tắc.

   b. Từ danh sách thả xuống **Lọc nội dung**, chọn tùy chọn được yêu cầu:

   - **Bất kỳ nội dung**.
   - **Theo danh mục nội dụng**.
   - **Theo loại dữ liệu**.
   - **Theo danh mục nội dung và loại dữ liệu**.

   c. Nếu một tùy chọn ngoài **Bất kỳ nội dung** được lựa chọn, các mục sẽ được mở ra cho hạng mục nội dung và / hoặc kiểu dữ liệu được lựa chọn. Chọn hộp kiểm cạnh tên của hạng mục nội dung và /

hoặc kiểu dữ liệu được lựa chọn.

Việc lựa chọn hộp kiểm cạnh tên của một hạng mục nội dung và / hoặc kiểu dữ liệu đồng nghĩa với việc Kaspersky Endpoint Security sẽ áp dụng quy tắc kiểm soát truy cập đến các tài nguyên web thuộc hạng mục nội dung và / hoặc kiểu dữ liệu được lựa chọn.

d. Từ danh sách thả xuống **Áp dụng cho địa chỉ**, chọn tùy chọn được yêu cầu:

- **Đến tất cả các địa chỉ**.
- **Đến các địa chỉ được chỉ định**.

e. Nếu tùy chọn **Đến các địa chỉ được chỉ định** được lựa chọn, một mục sẽ được mở ra, ở đó bạn có thể tạo một danh sách các tài nguyên web. Bạn có thể bổ sung hoặc sửa các địa chỉ tài nguyên web bằng cách sử dụng các nút **Thêm**, **Chỉnh sửa**, và **Gỡ bỏ**.

f. Chọn hộp kiểm **Chỉ định người dùng và / hoặc nhóm**.

g. Nhấn nút **Lựa chọn**.

Cửa sổ **Chọn Người dùng hoặc Nhóm Người dùng** trong Microsoft Windows sẽ được mở ra.

h. Quy định hoặc sửa danh sách người dùng và / hoặc nhóm người dùng được phép hoặc bị chặn truy cập đến các tài nguyên web được mô tả trong quy tắc.

i. Từ danh sách thả xuống **Hành động**, chọn tùy chọn được yêu cầu:

- **Cho phép** Nếu giá trị này được lựa chọn, Kaspersky Endpoint Security sẽ cho phép truy cập đến các tài nguyên web khớp với các tham số của quy tắc.
- **Ngăn chặn** Nếu giá trị này được lựa chọn, Kaspersky Endpoint Security sẽ chặn truy cập đến các tài nguyên web khớp với các tham số của quy tắc.
- **Cảnh báo**. Nếu giá trị này được lựa chọn, Kaspersky Endpoint Security sẽ hiển thị cảnh báo rằng một tài nguyên web là không mong muốn khi người dùng cố gắng truy cập các tài nguyên web khớp với quy tắc. Qua việc sử dụng các liên kết trong cảnh báo, người dùng có thể yêu cầu quyền truy cập đến tài nguyên web này.

j. Trong danh sách thả xuống **Quy tắc lập lịch**, chọn tên của lịch cần thiết hoặc tạo một lịch mới dựa trên lịch quy tắc được lựa chọn. Để làm điều này:

1. Đối diện danh sách thả xuống **Quy tắc lập lịch**, nhấn nút **Cấu hình**.

   Cửa sổ **Quy tắc lập lịch** sẽ được mở ra.

2. Để thêm một khoảng thời gian vào lịch quy tắc mà trong đó quy tắc không được áp dụng, trong bảng hiển thị lịch quy tắc, nhấn vào ô trong bảng tương ứng với thời gian và ngày trong tuần mà bạn muốn lựa chọn.

   Màu sắc của ô sẽ chuyển sang màu xám.

3. Để thay thế một khoảng thời gian trong đó quy tắc được áp dụng với một khoảng thời gian mà trong đó quy tắc không được áp dụng, nhấn vào ô màu xám trong bảng tương ứng với thời gian và ngày trong tuần mà bạn muốn lựa chọn.

   Màu sắc của ô sẽ chuyển sang màu xanh.

4. Nhấp vào nút **Lưu dưới dạng**.

   Cửa sổ **Tên quy tắc lập lịch** sẽ được mở ra.

5. Nhập một tên của lịch quy tắc hoặc sử dụng tên mặc định được đề xuất.

6. Nhấn **OK**.

5. Trong cửa sổ **Quy tắc truy cập tài nguyên web**, nhấn **OK**.

6. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Gán ưu tiên cho các quy tắc truy cập tài nguyên web

Bạn có thể gán mức độ ưu tiên cho mỗi quy tắc từ danh sách các quy tắc bằng cách sắp xếp các quy tắc theo thứ tự nhất định.

Để gán một mức độ ưu tiên cho một quy tắc truy cập tài nguyên web:

1. Mở cửa sổ cấu hình ứng dụng.

2. Ở phần bên trái của cửa sổ, trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát web**.
   Ở phần bên phải của cửa sổ, cấu hình của thành phần Kiểm soát web sẽ được hiển thị.

3. Ở phần bên phải của cửa sổ, chọn quy tắc mà bạn muốn thay đổi mức độ ưu tiên.

4. Sử dụng các nút **Di chuyển lên** và **Di chuyển xuống** để di chuyển quy tắc đến xếp hạng cần thiết trong danh sách quy tắc.

5. Lặp lại các bước 3–4 cho những quy tắc có mức độ ưu tiên mà bạn muốn thay đổi.

6. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Kiểm tra các quy tắc truy cập tài nguyên web

Để xác định tính nhất quán của các quy tắc Kiểm soát web, bạn có thể kiểm tra chúng. Vì mục đích này, thành phần Kiểm soát web có bao gồm một chức năng Chẩn đoán Quy tắc.

Để kiểm tra các quy tắc truy cập tài nguyên web:

1. Mở cửa sổ cấu hình ứng dụng.

2. Ở phần bên trái của cửa sổ, trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát web**.
   Ở phần bên phải của cửa sổ, cấu hình của thành phần Kiểm soát web sẽ được hiển thị.

3. Ở phía bên phải của cửa sổ, bấm vào nút **Chẩn đoán**.
   Cửa sổ **Chẩn đoán quy tắc** sẽ được mở ra.

4. Nhập vào các trường trong mục **Các điều kiện**:

   a. Nếu bạn muốn kiểm tra các quy tắc mà Kaspersky Endpoint Security sử dụng để kiểm soát truy cập đến một tài nguyên web cụ thể, chọn hộp kiểm **Chỉ định địa chỉ**. Nhập địa chỉ của tài nguyên web vào trường bên dưới.

b. Nếu bạn muốn kiểm tra các quy tắc mà Kaspersky Endpoint Security sử dụng để kiểm soát truy cập đến các tài nguyên web cho những người dùng và / hoặc nhóm người dùng được quy định, nhập một danh sách người dùng và / hoặc nhóm người dùng.

c. Nếu bạn muốn kiểm tra các quy tắc mà Kaspersky Endpoint Security sử dụng để kiểm soát truy cập đến các tài nguyên web của các hạng mục nội dung và / hoặc hạng mục kiểu dữ liệu cụ thể, từ danh sách thả xuống **Lọc nội dung**, chọn tùy chọn được yêu cầu (**Theo danh mục nội dụng**, **Theo loại dữ liệu**, hoặc **Theo danh mục nội dung và loại dữ liệu**).

d. Nếu bạn muốn kiểm tra quy tắc có xét đến thời gian và ngày trong tuần xảy ra một nỗ lực truy cập tài nguyên web được quy định trong điều kiện chẩn đoán quy tắc, hãy chọn hộp kiểm **Bao gồm thời gian cố gắng truy cập**. Sau đó quy định ngày trong tuần và thời gian.

5. Nhấn nút **Kiểm tra**.

Kiểm tra sẽ được hoàn thiện với thông tin về hành động được thực hiện bởi Kaspersky Endpoint Security, theo quy tắc đầu tiên được kích hoạt khi có nỗ lực truy cập tài nguyên web được quy định (cho phép, chặn hoặc cảnh báo). Quy tắc đầu tiên được kích hoạt là quy tắc có thứ hạng trên danh sách quy tắc Kiểm soát web cao hơn các quy tắc khác đáp ứng được điều kiện chẩn đoán. Thông tin này được hiển thị ở bên phải của nút **Kiểm tra**. Bảng sau liệt kê các quy tắc khác cũng bị kích hoạt, quy định hành động được thực thi bởi Kaspersky Endpoint Security. Các quy tắc được liệt kê theo thứ tự ưu tiên giảm dần.

Bật và tắt một quy tắc truy cập tài nguyên web

Để bật hoặc tắt một quy tắc truy cập tài nguyên web:

1. Mở cửa sổ cấu hình ứng dụng.
2. Ở phần bên trái của cửa sổ, trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát web**.
   Ở phần bên phải của cửa sổ, cấu hình của thành phần Kiểm soát web sẽ được hiển thị.
3. Ở phần bên phải của cửa sổ, chọn quy tắc mà bạn muốn bật hoặc tắt.
4. Trong cột **Trạng thái**, thực hiện các thao tác sau:
   - Nếu bạn muốn bật quy tắc, chọn giá trị *Bật*.
   - Nếu bạn muốn tắt quy tắc, chọn giá trị *Tắt*.
5. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Di chuyển quy tắc truy cập tài nguyên web từ phiên bản cũ của ứng dụng

Khi Service Pack 1 Maintenance Release 1 hoặc một phiên bản cũ của ứng dụng được nâng cấp lên Kaspersky Endpoint Security 10 Service Pack 2 for Windows, quy tắc truy cập tài nguyên web dựa trên hạng mục nội dung tài nguyên web sẽ được di chuyển như sau:

- Quy tắc truy cập tài nguyên web dựa trên một hoặc nhiều hạng mục nội dung tài nguyên web từ danh sách "Diễn đàn và tán gẫu", "Email trên web" và "Mạng xã hội" sẽ được di chuyển đến hạng mục nội dung tài nguyên web "Phương tiện truyền thông Internet".

- Quy tắc truy cập tài nguyên web dựa trên một hoặc nhiều hạng mục nội dung tài nguyên web từ danh sách "Cửa hàng điện tử" và "Hệ thống thanh toán" sẽ được di chuyển đến hạng mục nội dung tài nguyên web "Thương mại điện tử".
- Quy tắc truy cập tài nguyên web dựa trên hạng mục nội dung tài nguyên web "Cờ bạc" sẽ được di chuyển đến hạng mục nội dung "Cờ bạc, xổ số, rút thăm trúng thưởng".
- Quy tắc truy cập tài nguyên web dựa trên hạng mục nội dung tài nguyên web "Trò chơi trên trình duyệt" sẽ được di chuyển đến hạng mục nội dung "Trò chơi điện tử".
- Quy tắc truy cập tài nguyên web dựa trên các hạng mục nội dung tài nguyên web không được liệt kê trong danh sách trên sẽ được di chuyển mà không thay đổi gì.

Xuất và nhập danh sách địa chỉ tài nguyên web

Nếu bạn đã tạo một danh sách các địa chỉ tài nguyên web trong một quy tắc truy cập tài nguyên web, bạn có thể xuất nó ra một tập tin .txt. Sau đó, bạn có thể nhập danh sách từ tập tin này để tránh tạo một danh sách các địa chỉ tài nguyên web mới một cách thủ công khi thiết lập một quy tắc truy cập. Tùy chọn xuất và nhập danh sách các địa chỉ tài nguyên web có thể là hữu ích nếu, chẳng hạn, bạn tạo ra các quy tắc truy cập có tham số giống nhau.

Để xuất một danh sách các địa chỉ tài nguyên web ra một tập tin:

1. Mở cửa sổ cấu hình ứng dụng.
2. Ở phần bên trái của cửa sổ, trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát web**.
   Ở phần bên phải của cửa sổ, cấu hình của thành phần Kiểm soát web sẽ được hiển thị.
3. Chọn quy tắc có danh sách địa chỉ tài nguyên web mà bạn muốn xuất ra một tập tin.
4. Nhấn nút **Chỉnh sửa**.
   Cửa sổ **Quy tắc truy cập tài nguyên web** sẽ được mở ra.
5. Nếu bạn không muốn xuất toàn bộ danh sách địa chỉ tài nguyên web, mà chỉ một phần của nó, hãy chọn các địa chỉ tài nguyên web cần thiết.
6. Ở bên phải của trường với danh sách địa chỉ tài nguyên web, nhấn nút  .
   Cửa sổ xác nhận hành động sẽ được mở ra.
7. Thực hiện một trong các thao tác sau:
   - Nếu bạn chỉ muốn xuất các đề mục được chọn trong danh sách địa chỉ tài nguyên web, trong cửa sổ xác nhận hành động, nhấn nút **Có**.
   - Nếu bạn muốn xuất tất cả các mục trong danh sách địa chỉ tài nguyên web, trong cửa sổ xác nhận hành động, nhấn nút **Không**.
     Cửa sổ **Lưu dưới dạng** tiêu chuẩn của Microsoft Office sẽ được mở ra.
8. Trong cửa sổ **Lưu dưới dạng** của Microsoft Windows, chọn tập tin mà bạn muốn xuất danh sách địa chỉ tài nguyên web vào đó. Nhấp vào nút **Lưu**.

Để nhập danh sách các địa chỉ tài nguyên web từ một tập tin vào một quy tắc:

1. Mở cửa sổ cấu hình ứng dụng.
2. Ở phần bên trái của cửa sổ, trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát web**.
   Ở phần bên phải của cửa sổ, cấu hình của thành phần Kiểm soát web sẽ được hiển thị.
3. Thực hiện một trong các thao tác sau:
   - Nếu bạn muốn tạo một quy tắc truy cập tài nguyên web mới, nhấn nút **Thêm**.
   - Chọn quy tắc truy cập tài nguyên web mà bạn muốn sửa. Sau đó nhấn nút **Chỉnh sửa**.

   Cửa sổ **Quy tắc truy cập tài nguyên web** sẽ được mở ra.
4. Thực hiện một trong các thao tác sau:
   - Nếu bạn đang tạo một quy tắc truy cập tài nguyên web mới, chọn **Đến các địa chỉ được chỉ định** từ danh sách thả xuống **Áp dụng cho địa chỉ**.
   - Nếu bạn đang sửa một quy tắc truy cập tài nguyên web, đến bước 5 của các chỉ dẫn này.
5. Ở bên phải của trường với danh sách địa chỉ tài nguyên web, nhấn nút .
   Nếu bạn đang tạo một quy tắc mới, cửa sổ **Mở tập tin** tiêu chuẩn của Microsoft Windows sẽ được mở ra.
   Nếu bạn đang sửa một quy tắc, một cửa sổ yêu cầu xác nhận của bạn sẽ được mở ra.
6. Thực hiện một trong các thao tác sau:
   - Nếu bạn đang sửa một quy tắc truy cập tài nguyên web mới, đến bước 7 của các chỉ dẫn này.
   - Nếu bạn đang sửa một quy tắc truy cập tài nguyên web, thực hiện một trong các hành động sau trong cửa sổ xác nhận hành động:
     - Nếu bạn muốn thêm các đề mục nhập từ danh sách địa chỉ tài nguyên web vào một danh sách hiện tại, nhấn nút **Có**.
     - Nếu bạn muốn xóa các đề mục hiện tại của danh sách địa chỉ tài nguyên web và bổ sung các đề mục nhập, nhấn nút **Không**.

   Cửa sổ **Mở tập tin** trong Microsoft Windows sẽ được mở ra.
7. Trong cửa sổ **Mở tập tin** của Microsoft Windows, chọn một tập tin có danh sách các địa chỉ tài nguyên web để nhập.
8. Nhấn nút **Mở**.
9. Trong cửa sổ **Quy tắc truy cập tài nguyên web**, nhấn **OK**.

Sửa mặt nạ cho các địa chỉ tài nguyên web

Việc sử dụng một *mặt nạ địa chỉ tài nguyên web* (còn được gọi là một "mặt nạ địa chỉ") có thể là hữu ích nếu bạn cần nhập nhiều địa chỉ tài nguyên web giống nhau khi tạo một quy tắc truy cập tài nguyên web. Nếu được viết tốt, một mặt nạ địa chỉ có thể thay thế một lượng lớn các địa chỉ tài nguyên web.

Khi tạo một mặt nạ địa chỉ, cần tuân theo các quy tắc sau đây:

1. Ký tự * thay thế bất kỳ chuỗi ký tự nào chứa từ 0 ký tự hoặc hơn.

   Ví dụ, nếu bạn nhập mặt nạ địa chỉ *abc*, quy tắc truy cập sẽ được áp dụng cho mọi tài nguyên web có chứa chuỗi abc. Ví dụ: http://www.example.com/page_0-9abcdef.html.

   Để bao gồm ký tự * trong mặt nạ địa chỉ, nhập ký tự * hai lần.

2. Chuỗi ký tự `www.` ở đầu mặt nạ địa chỉ được diễn giải như một chuỗi `*.`.

   Ví dụ: mặt nạ địa chỉ www.example.com được coi như là *.example.com.

3. Nếu một mặt nạ địa chỉ không bắt đầu với ký tự *, nội dung của mặt nạ địa chỉ sẽ tương đương với cùng nội dung có tiền tố `*.` .

4. Chuỗi ký tự `*.` ở đầu một mặt nạ địa chỉ sẽ được diễn giải như là `*.` hoặc một chuỗi rỗng.

   Ví dụ: mặt nạ địa chỉ http://www.*.example.com bao gồm địa chỉ http://www2.example.com.

5. Nếu một mặt nạ địa chỉ kết thúc với một ký tự ngoài `/` hoặc *, nội dung của mặt nạ địa chỉ sẽ tương đương với cùng một nội dung có hậu tố `/*`.

   Ví dụ: mặt nạ địa chỉ http://www.example.com cũng bao gồm các địa chỉ như http://www.example.com/abc, mà ở đó a, b, và c là các ký tự bất kỳ.

6. Nếu một mặt nạ địa chỉ kết thúc với ký tự /, nội dung của mặt nạ địa chỉ sẽ tương đương với cùng một nội dung có hậu tố `/*.` .

7. Chuỗi ký tự `/*` ở cuối một mặt nạ địa chỉ sẽ được diễn giải như là `/*` hoặc một chuỗi rỗng.

8. Các địa chỉ tài nguyên web sẽ được đối chiếu với một mặt nạ địa chỉ, có xét đến giao thức (http hoặc https):

   - Nếu một mặt nạ địa chỉ không chứa bất kỳ giao thức mạng nào, mặt nạ địa chỉ này sẽ bao gồm các địa chỉ có một giao thức mạng bất kỳ.

     Ví dụ: mặt nạ địa chỉ example.com cũng bao gồm các địa chỉ http://example.com và https://example.com.

   - Nếu mặt nạ địa chỉ có chứa một giao thức mạng, mặt nạ địa chỉ này sẽ chỉ bao gồm các địa chỉ có cùng giao thức mạng với mặt nạ địa chỉ đó.

     Ví dụ: mặt nạ địa chỉ http://*.example.com bao gồm địa chỉ http://www.example.com nhưng không bao gồm https://www.example.com.

9. Một mặt nạ địa chỉ được đặt trong ngoặc kép được coi là không có bất kỳ địa chỉ thay thế nào khác, ngoại trừ ký tự * nếu ban đầu nó được bao gồm trong mặt nạ địa chỉ. Quy tắc 5 và 7 không áp dụng cho các mặt nạ địa chỉ được đặt trong ngoặc kép (xem các ví dụ 14 – 18 trong bảng dưới đây).

10. Tên người dùng và mật khẩu, cổng kết nối, và dạng chữ hoa/chữ thường của ký tự sẽ không được xét đến khi đối chiếu với mặt nạ địa chỉ của một tài nguyên web.

Các ví dụ về cách để sử dụng quy tắc cho việc tạo mặt nạ địa chỉ

Không.	Mặt nạ địa chỉ	Địa chỉ tài nguyên web cần kiểm chứng	Địa chỉ này có được bao gồm trong mặt nạ	Nhận xét

			địa chỉ không	
1	*.example.com	http://www.123example.com	Không	Xem quy tắc 1.
2	*.example.com	http://www.123.example.com	Có	Xem quy tắc 1.
3	*example.com	http://www.123example.com	Có	Xem quy tắc 1.
4	*example.com	http://www.123.example.com	Có	Xem quy tắc 1.
5	http://www.*.example.com	http://www.123example.com	Không	Xem quy tắc 1.
6	www.example.com	http://www.example.com	Có	Xem các quy tắc 2, 1.
7	www.example.com	https://www.example.com	Có	Xem các quy tắc 2, 1.
8	http://www.*.example.com	http://123.example.com	Có	Xem các quy tắc 2, 4, 1.
9	www.example.com	http://www.example.com/abc	Có	Xem các quy tắc 2, 5, 1.
10	example.com	http://www.example.com	Có	Xem các quy tắc 3, 1.
11	http://example.com/	http://example.com/abc	Có	Xem quy tắc 6.
12	http://example.com/*	http://example.com	Có	Xem quy tắc 7.
13	http://example.com	https://example.com	Không	Xem quy tắc 8.
14	"example.com"	http://www.example.com	Không	Xem quy tắc 9.
15	"http://www.example.com"	http://www.example.com/abc	Không	Xem quy tắc 9.
16	"*.example.com"	http://www.example.com	Có	Xem các quy tắc 1, 9.
17	"http://www.example.com/*"	http://www.example.com/abc	Có	Xem các quy tắc 1, 9.
18	"www.example.com"	http://www.example.com; https://www.example.com	Có	Xem các quy tắc 9, 8.
19	www.example.com/abc/123	http://www.example.com/abc	Không	Một mặt nạ địa chỉ

				chứa nhiều thông tin hơn địa chỉ của một tài nguyên web.

Sửa mẫu thông điệp Kiểm soát web

Tùy thuộc vào kiểu hành động được quy định trong thuộc tính của các quy tắc Kiểm soát web, Kaspersky Endpoint Security sẽ hiển thị một thông điệp về một trong những kiểu hành động sau đây khi người dùng cố gắng truy cập các tài nguyên Internet (ứng dụng sẽ thay thế một trang HTML với một thông điệp phản hồi từ máy chủ HTTP):

- Thông điệp cảnh báo. Thông điệp này sẽ cảnh báo với người dùng rằng việc truy cập tài nguyên web này là không được khuyến khích và / hoặc vi phạm chính sách bảo mật doanh nghiệp. Kaspersky Endpoint Security sẽ hiển thị một thông điệp cảnh báo nếu tùy chọn **Cảnh báo** được chọn từ danh sách thả xuống **Hành động** trong cấu hình quy tắc mô tả tài nguyên web này.

  Nếu người dùng tin rằng cảnh báo này là nhầm lẫn, người dùng có thể nhấn vào liên kết trong cảnh báo để gửi một thông điệp được tạo sẵn đến quản trị viên mạng doanh nghiệp cục bộ.

- Thông điệp báo cáo việc chặn một tài nguyên web. Kaspersky Endpoint Security hiển thị thông điệp rằng một tài nguyên web sẽ bị chặn nếu tùy chọn **Ngăn chặn** được chọn từ danh sách thả xuống **Hành động** trong cấu hình quy tắc mô tả tài nguyên web này.

  Nếu người dùng tin rằng tài nguyên web này đã bị chặn nhầm, người dùng có thể nhấn vào liên kết trong thông điệp chặn tài nguyên web để gửi một thông điệp được tạo sẵn đến quản trị viên mạng doanh nghiệp cục bộ.

Các mẫu đặc biệt cũng được cung cấp cho thông điệp cảnh báo, thông điệp rằng một tài nguyên web đã bị chặn, và thông điệp được gửi đến quản trị viên mạng LAN. Bạn có thể sửa nội dung của chúng.

Để thay đổi mẫu thông điệp Kiểm soát web:

1. Mở cửa sổ cấu hình ứng dụng.

2. Ở phần bên trái của cửa sổ, trong mục **Bảng kiểm soát**, chọn mục con **Kiểm soát web**.

   Ở phần bên phải của cửa sổ, cấu hình của thành phần Kiểm soát web sẽ được hiển thị.

3. Ở phía bên phải của cửa sổ, bấm vào nút **Mẫu**.

   Cửa sổ **Tin nhắn mẫu** sẽ được mở ra.

4. Thực hiện một trong các thao tác sau:

   - Nếu bạn muốn sửa mẫu thông điệp cảnh báo người dùng về việc truy cập một tài nguyên web, chọn thẻ **Cảnh báo**.

   - Nếu bạn muốn sửa mẫu thông điệp báo rằng việc truy cập đến một tài nguyên web đã bị chặn, chọn thẻ **Thông báo**.

- Để sửa mẫu thông điệp được gửi đến quản trị viên, chọn thẻ **Thông điệp đến quản trị viên**.

5. Sửa mẫu thông điệp. Bạn cũng có thể sử dụng danh sách thả xuống **Biến số**, cũng như các nút **Mặc định** và **Liên kết** (nút này không khả dụng trên thẻ **Thông điệp đến quản trị viên**).

6. Nhấn **OK**.

7. Để lưu lại các thay đổi, nhấn nút **Lưu**.

KATA Endpoint Sensor

Cấu hình của thành phần KATA Endpoint Sensor chỉ khả dụng trong Bảng điều khiển Quản trị Kaspersky Security Center. Để sử dụng thành phần này, bạn phải cài đặt tiện ích quản trị.

Mục này chứa thông tin về KATA Endpoint Sensor và chỉ dẫn cách để bật hoặc tắt thành phần này.

Thông tin về KATA Endpoint Sensor

KATA Endpoint Sensor là một thành phần của Kaspersky Anti Targeted Attack Platform. Giải pháp này được thiết kế để phát hiện nhanh các mối đe dọa như các cuộc tấn công có mục tiêu.

Thành phần này được cài đặt trên các máy khách. Trên các máy tính này, thành phần này sẽ liên tục giám sát các tiến trình, kết nối mạng hoạt động, và các tập tin được sửa đổi, và chuyển tiếp thông tin này đến Kaspersky Anti Targeted Attack Platform.

Chức năng thành phần này có thể được sử dụng trong các hệ điều hành sau:

- Microsoft Windows 7 Professional / Enterprise / Ultimate x86 Edition SP1, Microsoft Windows 7 Professional / Enterprise / Ultimate x64 Edition SP1
- Microsoft Windows 8.1 Enterprise x86 Edition, Microsoft Windows 8.1 Enterprise x64 Edition.
- Microsoft Windows 10 Pro / Enterprise x86 Edition, Microsoft Windows 10 Pro / Enterprise x64 Edition.
- Microsoft Windows Server 2008 R2 Standard / Enterprise x64 Edition SP1.
- Microsoft Windows Server 2012 Standard / Foundation / Essentials x64 Edition, Microsoft Windows Server 2012 R2 Standard / Foundation / Essentials x64 Edition.
- Microsoft Windows Server 2016

Để biết thêm thông tin về Kaspersky Anti Targeted Attack Platform không có trong tài liệu này, vui lòng tham khảo phần trợ giúp của Kaspersky Anti Targeted Attack Platform.

Các kết nối vào máy tính có thành phần KATA Endpoint Sensor phải được cho phép từ chính Kaspersky Anti Targeted Attack Platform, mà không có máy chủ proxy.

Bật và tắt thành phần KATA Endpoint Sensor

Để bật hoặc tắt thành phần KATA Endpoint Sensor:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, mở thư mục với tên của nhóm quản trị mà bạn muốn sửa cấu hình chính sách.

3. Trong không gian làm việc, chọn thẻ **Chính sách**.

4. Chọn chính sách cần thiết.

5. Mở cửa sổ **Thuộc tính: <Tên chính sách>** sử dụng một trong những phương pháp sau đây:

   - Trong menu ngữ cảnh của chính sách, chọn **Thuộc tính**.
   - Nhấn vào liên kết **Thiết lập chính sách** được đặt ở phần bên phải của không gian làm việc của Bảng điều khiển Quản trị.

6. Trong mục **Cấu hình nâng cao**, chọn mục con **KATA Endpoint Sensor**.

7. Thực hiện một trong các thao tác sau:

   - Nếu bạn muốn bật KATA Endpoint Sensor, chọn hộp kiểm **KATA Endpoint Sensor**.
   - Nếu bạn muốn tắt KATA Endpoint Sensor, xóa hộp kiểm **KATA Endpoint Sensor**.

8. Nếu bạn đã chọn hộp kiểm **KATA Endpoint Sensor** ở bước trước, trong trường **Địa chỉ máy chủ**, nhập địa chỉ máy chủ của Kaspersky Anti Targeted Attack Platform gồm các phần sau:

   a. Tên giao thức

   b. Địa chỉ IP hoặc một tên miền đủ tiêu chuẩn (FQDN) của máy chủ

   c. Đường dẫn đến Windows Event Collector trên máy chủ

9. Nhấn **OK**.

10. Áp dụng chính sách.

    Xem *Hướng dẫn dành cho Quản trị viên Kaspersky Security Center* để biết chi tiết về việc áp dụng các chính sách Kaspersky Security Center.

Mã hóa Dữ liệu

Nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Microsoft Windows for Workstations, toàn bộ chức năng mã hóa dữ liệu sẽ có thể được sử dụng. Nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Microsoft Windows cho Máy chủ Tập tin, chỉ chức năng mã hóa ổ cứng sử dụng công nghệ BitLocker Drive Encryption là có thể được sử dụng.

Mục này chứa thông tin về việc mã hóa và giải mã các ổ cứng, ổ đĩa di động, các tập tin và thư mục trên ổ đĩa của máy tính cục bộ, và cung cấp chỉ dẫn về cách để thiết lập và thực hiện tác vụ mã hóa và giải mã dữ liệu sử dụng Kaspersky Endpoint Security và tiện ích quản trị Kaspersky Endpoint Security.

Nếu không thể truy cập dữ liệu được mã hóa, hãy xem chỉ dẫn đặc biệt khi làm việc với dữ liệu được mã hóa (Làm việc với các tập tin được mã hóa trong trường hợp chức năng mã hóa tập tin bị hạn chế, Làm việc với các thiết bị được mã hóa trong trường hợp không thể truy cập chúng).

Bật hiển thị cấu hình mã hóa trong chính sách Kaspersky Security Center

Để bật hiển thị cấu hình mã hóa trong chính sách Kaspersky Security Center:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Trong menu ngữ cảnh của nút **Máy chủ Quản trị – <Tên máy tính>** của cây Bảng điều khiển Quản trị, chọn thẻ **Xem → Cấu hình giao diện**.

   Cửa sổ **Cấu hình giao diện** sẽ được mở ra.
3. Trong cửa sổ **Cấu hình giao diện**, chọn hộp kiểm **Hiển thị mã hóa và bảo vệ dữ liệu**.
4. Nhấn **OK**.

Thông tin về mã hóa dữ liệu

Kaspersky Endpoint Security cho phép bạn mã hóa các tập tin và thư mục được lưu trữ trên các ổ đĩa cục bộ và ổ đĩa di động, cũng như toàn bộ các ổ cứng và ổ đĩa di động. Việc mã hóa dữ liệu giúp giảm thiểu nguy cơ rò rỉ thông tin khi một máy tính lưu động, ổ đĩa di động hoặc ổ cứng bị thất lạc hoặc mất cắp, hoặc khi dữ liệu được truy cập bởi những người dùng hoặc ứng dụng trái phép.

Nếu giấy phép đã hết hạn, ứng dụng sẽ không thể mã hóa dữ liệu mới, và các dữ liệu được mã hóa cũ vẫn sẽ duy trì tình trạng mã hóa và có thể được sử dụng. Trong trường hợp này, việc mã hóa dữ liệu mới đòi hỏi chương trình được kích hoạt với một giấy phép mới cho phép việc sử dụng mã hóa.

Nếu giấy phép của bạn đã hết hạn, hoặc Thỏa thuận Giấy phép Người dùng Cuối đã bị vi phạm, hoặc khóa hay Kaspersky Endpoint Security hoặc thành phần mã hóa đã bị gỡ bỏ, trạng thái mã hóa của các tập tin được mã hóa từ trước sẽ không được bảo đảm. Điều này là bởi vì một số ứng dụng, ví dụ như Microsoft Office Word sẽ tạo một bản sao tạm thời của các tập tin trong quá trình chỉnh sửa. Khi tập tin gốc được lưu lại, bản sao tạm thời sẽ thay thế tập tin gốc. Kết quả là, trên một máy tính không có hoặc không thể truy cập chức năng mã hóa, tập tin vẫn ở tình trạng chưa được mã hóa.

Kaspersky Endpoint Security cung cấp các khía cạnh bảo vệ dữ liệu sau:

- **Mã hóa các tập tin trên ổ đĩa cục bộ trên máy tính**. Bạn có thể tổng hợp danh sách các tập tin theo phần mở rộng hoặc nhóm phần mở rộng và danh sách thư mục được lưu trữ trên các ổ đĩa máy tính cục bộ, và tạo các quy tắc mã hóa tập tin được tạo bởi các ứng dụng cụ thể. Sau khi một chính sách Kaspersky Security Center đã được áp dụng, Kaspersky Endpoint Security sẽ mã hóa và giải mã các tập tin sau:

  - Những tập tin đã được thêm lần lượt vào danh sách mã hóa và giải mã.
  - Những tập tin được lưu trữ trong các thư mục được thêm vào danh sách mã hóa và giải mã.
  - những tập tin được tạo bởi các ứng dụng riêng biệt.

  Xem *Hướng dẫn dành cho Quản trị viên Kaspersky Security Center* để biết chi tiết về việc áp dụng các chính sách Kaspersky Security Center.

- **Mã hóa ổ đĩa di động**. Bạn có thể quy định một quy tắc mã hóa mặc định mà theo đó ứng dụng sẽ áp dụng một hành động cho tất cả các ổ đĩa di động, hoặc quy định các quy tắc mã hóa cho những ổ đĩa di động riêng biệt.

  Quy tắc mã hóa mặc định có mức độ ưu tiên thấp hơn các quy tắc mã hóa được tạo cho các ổ đĩa di động riêng lẻ. Quy tắc mã hóa được tạo cho các ổ đĩa di động của một mẫu thiết bị cụ thể có mức độ ưu tiên thấp hơn các quy tắc mã hóa được tạo cho các ổ đĩa di động riêng lẻ có ID thiết bị cụ thể.

  Để chọn một quy tắc mã hóa cho các tập tin trên một ổ đĩa di động, Kaspersky Endpoint Security sẽ kiểm tra liệu mẫu thiết bị và ID đã được biết hay chưa. Sau đó, ứng dụng sẽ thực hiện một trong các hoạt động sau:

  - Nếu chỉ mẫu thiết bị là được biết, ứng dụng sẽ sử dụng quy tắc mã hóa (nếu có) được tạo cho các ổ đĩa di động của mẫu thiết bị cụ thể.
  - Nếu chỉ ID thiết bị là được biết, ứng dụng sẽ sử dụng quy tắc mã hóa (nếu có) được tạo cho các ổ đĩa di động với ID thiết bị cụ thể.
  - Nếu cả mẫu và ID thiết bị đều được biết, ứng dụng sẽ áp dụng quy tắc mã hóa (nếu có) được tạo cho các ổ đĩa di động với ID thiết bị cụ thể. Nếu không tồn tại quy tắc nào như vậy, nhưng có một quy tắc mã hóa được tạo cho các ổ đĩa di động với mẫu thiết bị cụ thể, ứng dụng sẽ áp dụng quy tắc này. Nếu không có quy tắc mã hóa nào được quy định cho ID thiết bị cụ thể hay cho mẫu thiết bị cụ thể, ứng dụng sẽ áp dụng quy tắc mã hóa mặc định.
  - Nếu cả mẫu thiết bị và ID thiết bị đều không được biết, ứng dụng sẽ sử dụng quy tắc mã hóa mặc định.

  Ứng dụng cho phép bạn chuẩn bị một ổ đĩa di động cho việc sử dụng dữ liệu được mã hóa trên đó trong chế độ lưu động. Sau khi đã bật chế độ lưu động, bạn có thể truy cập các tập tin được mã hóa trên ổ đĩa di động được kết nối đến một máy tính không có chức năng mã hóa.

  Ứng dụng sẽ thực hiện hành động được quy định trong quy tắc mã hóa khi chính sách Kaspersky Security Center được áp dụng.

- **Quản lý các quy tắc truy cập tập tin được mã hóa của ứng dụng**. Với bất kỳ ứng dụng nào, bạn cũng có thể tạo một quy tắc truy cập tập tin được mã hóa chặn truy cập đến các tập tin được mã hóa, hoặc cho phép truy cập đến các tập tin được mã hóa dưới dạng văn bản mật mã, là một chuỗi ký tự nhận được khi áp dụng mã hóa.

- **Tạo các tập nén được mã hóa**. Bạn có thể tạo các tập nén được mã hóa và bảo vệ truy cập đến các tập nén đó với một mật khẩu. Nội dung của các tập nén được mã hóa chỉ có thể được truy cập bằng cách nhập mật khẩu được bạn sử dụng để bảo vệ việc truy cập đến các tập nén này. Các tập nén này có thể được truyền tải bảo mật qua mạng hoặc trên ổ đĩa di động.

- **Mã hóa ổ cứng**. Bạn có thể chọn một công nghệ mã hóa: Kaspersky Disk Encryption hoặc Mã hóa Ổ đĩa BitLocker (sau đây cũng được gọi tắt là "BitLocker").

  BitLocker là một công nghệ trong hệ điều hành Windows. Nếu máy tính được trang bị một Mô-đun Nền tảng Đáng Tin cậy (TPM), BitLocker sẽ sử dụng nó để lưu các khóa khôi phục cho phép truy cập đến một ổ cứng được mã hóa. Khi máy tính được khởi động, BitLocker sẽ yêu cầu khóa khôi phục ổ cứng từ Mô-đun Nền tảng Đáng Tin cậy và mở khóa ổ đĩa này. Bạn có thể thiết lập việc sử dụng mật khẩu và / hoặc mã PIN để truy cập các khóa khôi phục.

  Bạn có thể quy định quy tắc mã hóa ổ cứng mặc định và tạo một danh sách ổ cứng được loại trừ khỏi tác vụ mã hóa. Kaspersky Endpoint Security sẽ thực hiện mã hóa ổ cứng theo từng khu vực sau khi chính sách Kaspersky Security Center được áp dụng. Công nghệ này sẽ mã hóa tất cả các phân vùng lôgic của ổ cứng cùng một lúc. Xem *Hướng dẫn dành cho Quản trị viên Kaspersky Security Center* để biết chi tiết về việc áp dụng các chính sách Kaspersky Security Center.

  Sau khi ổ cứng hệ thống đã được mã hóa, vào lần khởi động tiếp theo, người dùng sẽ phải hoàn tất xác thực sử dụng Authentication Agent trước khi ổ cứng có thể được truy cập và hệ điều hành có thể được nạp. Điều này đòi hỏi bạn nhập vào mật khẩu của token hoặc thẻ thông minh được kết nối đến máy tính, hoặc tên người dùng và mật khẩu của tài khoản Authentication Agent được tạo bởi quản trị viên mạng máy tính cục bộ sử dụng tác vụ quản lý tài khoản Authentication Agent. Những tài khoản này đều dựa trên các tài khoản Microsoft Windows được người dùng sử dụng để đăng nhập vào hệ điều hành. Bạn có thể quản lý các tài khoản Authentication Agent và sử dụng công nghệ Single Sign-On (SSO) cho phép bạn đăng nhập tự động vào hệ điều hành sử dụng tên người dùng và mật khẩu của tài khoản Authentication Agent.

  > Nếu bạn sao lưu một máy tính và sau đó mã hóa dữ liệu máy tính, sau đó khôi phục bản sao dự phòng của máy tính và mã hóa lại dữ liệu máy tính một lần nữa, Kaspersky Endpoint Security sẽ tạo các bản sao của tài khoản Authentication Agent. Để xóa các tài khoản trùng nhau, bạn phải sử dụng tiện ích klmover với khóa `dupfix`. Tiện ích klmover được bao gồm trong bản dựng của Kaspersky Security Center. Bạn có thể đọc thêm về hoạt động của tiện ích này trong *Hướng dẫn dành cho Quản trị viên Kaspersky Security Center*.

  > Khi phiên bản ứng dụng được nâng cấp lên Kaspersky Endpoint Security 10 Service Pack 2 for Windows, danh sách các tài khoản Authentication Agent sẽ không được lưu lại.

  Việc truy cập đến các ổ cứng được mã hóa sẽ chỉ có thể được thực hiện trên các máy tính có cài đặt Kaspersky Endpoint Security với chức năng mã hóa ổ cứng. Biện pháp phòng ngừa này giúp giảm thiểu nguy cơ rò rỉ dữ liệu từ một ổ cứng được mã hóa khi một nỗ lực truy cập nó được thực hiện từ bên ngoài mạng máy tính cục bộ của công ty.

Để mã hóa các ổ cứng và ổ đĩa di động, bạn có thể sử dụng chức năng **Chỉ mã hóa dung lượng ổ đĩa được sử dụng**. Bạn được khuyến nghị chỉ sử dụng chức năng này cho các thiết bị mới chưa được sử dụng trước đây. Nếu bạn đang áp dụng mã hóa cho một thiết bị đang được sử dụng, bạn nên mã hóa toàn bộ thiết bị đó. Điều này đảm bảo mọi dữ liệu đều được bảo vệ - kể cả những dữ liệu đã bị xóa có thể vẫn chứa thông tin truy hồi được.

Trước khi bắt đầu mã hóa, Kaspersky Endpoint Security sẽ nhận bản đồ các khu vực của hệ thống tập tin. Lượt mã hóa đầu tiên bao gồm các khu vực chứa tập tin tại thời điểm mã hóa được bắt đầu. Lượt mã hóa thứ hai bao gồm các khu vực được ghi sau khi quá trình mã hóa được bắt đầu. Sau khi quá trình mã hóa được hoàn tất, tất cả các khu vực chứa dữ liệu đều sẽ được mã hóa.

Sau khi quá trình mã hóa được hoàn tất và người dùng xóa một tập tin, các khu vực chứa tập tin bị xóa sẽ có thể được sử dụng để lưu trữ thông tin mới ở cấp hệ thống tập tin, nhưng vẫn được mã hóa. Vì vậy, khi các tập tin mới được ghi vào một thiết bị mới trong lúc khởi chạy mã hóa thông thường với chức năng **Chỉ mã hóa dung lượng ổ đĩa được sử dụng** được bật trên máy tính, sau một thời gian tất cả các phân vùng sẽ được mã hóa.

Dữ liệu cần thiết để giải mã các tập tin được cung cấp bởi Máy chủ Quản trị của Kaspersky Security Center kiểm soát máy tính tại thời điểm mã hóa. Nếu máy tính với các tập tin được mã hóa được chuyển sang sự kiểm soát của một Máy chủ Quản trị khác vì bất cứ lý do gì, và các tập tin được mã hóa chưa bao giờ được truy cập, quyền truy cập có thể được nhận bằng một trong các cách sau:

- yêu cầu truy cập đến các đối tượng được mã hóa từ quản trị viên mạng LAN;
- khôi phục dữ liệu trên các thiết bị được mã hóa sử dụng Tiện ích Khôi phục;
- Khôi phục thiết lập của Máy chủ Quản trị của Kaspersky Security Center đã kiểm soát máy tính tại thời điểm mã hóa từ một bản sao dự phòng và sử dụng thiết lập này trên Máy chủ Quản trị hiện đang kiểm soát máy tính có chứa các đối tượng được mã hóa.

Ứng dụng sẽ tạo các tập tin dịch vụ trong quá trình mã hóa. Cần khoảng 2% đến 3% không gian trống không phân mảnh trên ổ cứng để lưu trữ chúng. Nếu không có đủ không gian trống không phân mảnh trên ổ cứng, việc mã hóa sẽ không được bắt đầu cho đến khi đã giải phóng đủ không gian trống.

Sự tương thích giữa chức năng mã hóa của Kaspersky Endpoint Security và Kaspersky Anti-Virus cho UEFI là không được hỗ trợ. Việc mã hóa ổ cứng của các máy tính mà trên đó có cài đặt Kaspersky Anti-Virus cho UEFI sẽ khiến Kaspersky Anti-Virus cho UEFI không thể hoạt động được.

Hạn chế của chức năng mã hóa

Việc tạo phân vùng mới trên các ổ cứng được mã hóa hay định dạng lại phân vùng hiện tại của các ổ cứng được mã hóa có thể gây mất dữ liệu trên các ổ cứng này.

Mã hóa ổ cứng sử dụng công nghệ Kaspersky Disk Encryption sẽ không thể được sử dụng cho các ổ cứng không đáp ứng được yêu cầu về phần cứng và phần mềm.

Kaspersky Endpoint Security sẽ không hỗ trợ các thiết lập sau:

- Tiện ích nạp khởi động được đặt trên một ổ đĩa, còn hệ điều hành được đặt trên một ổ đĩa khác.
- Hệ thống chứa phần mềm nhúng thuộc chuẩn UEFI 32.
- Công nghệ Intel® Rapid Start Technology và các ổ đĩa có phân vùng ngủ đông, kể cả khi Intel® Rapid Start Technology đã bị tắt.
- Các ổ đĩa trong định dạng MBR với nhiều hơn bốn phân vùng mở rộng.
- Tập tin swap được đặt trên một ổ đĩa không phải ổ đĩa hệ thống.
- Hệ thống đa khởi động với nhiều hệ điều hành được cài đặt cùng nhau.
- Các phân vùng động (chỉ các phân vùng chính mới được hỗ trợ).
- Các ổ đĩa có dưới 2% không gian ổ đĩa không phân mảnh tự do.

- Các ổ đĩa có kích cỡ khu vực (sector) khác với 512 byte hoặc 4096 byte giả lập 512 byte.
- Các ổ đĩa lai.

Thay đổi thuật toán mã hóa

Thuật toán mã hóa được sử dụng bởi Kaspersky Endpoint Security để mã hóa dữ liệu tùy thuộc vào thư viện mã hóa được bao gồm trong gói phân phối.

Để thay đổi thuật toán mã hóa:

1. Giải mã các đối tượng được Kaspersky Endpoint Security mã hóa trước khi bắt đầu thay đổi thuật toán mã hóa.

   Sau khi thuật toán mã hóa đã được thay đổi, các đối tượng được mã hóa từ trước sẽ không thể được sử dụng.

2. Gỡ bỏ Kaspersky Endpoint Security.
3. Cài đặt Kaspersky Endpoint Security từ gói phân phối chứa các thư viện mã hóa cho các phiên bản bit khác nhau.

Bật công nghệ Single Sign-On (SSO)

Công nghệ Single Sign-On (SSO) không tương thích với các nhà cung cấp chứng chỉ tài khoản thuộc bên thứ ba.

Để bật công nghệ Single Sign-On (SSO):

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, mở thư mục với tên của nhóm quản trị mà bạn muốn bật công nghệ Single Sign-On (SSO).
3. Trong không gian làm việc, chọn thẻ **Chính sách**.
4. Chọn chính sách cần thiết.
5. Mở cửa sổ **Thuộc tính: <Tên chính sách>** sử dụng một trong những phương pháp sau đây:
   - Trong menu ngữ cảnh của chính sách, chọn **Thuộc tính**.
   - Nhấn vào liên kết **Thiết lập chính sách** được đặt ở phần bên phải của không gian làm việc của Bảng điều khiển Quản trị.
6. Trong mục **Mã hóa dữ liệu**, chọn mục con **Cấu hình mã hóa chung**.
7. Trong mục con **Cấu hình mã hóa chung**, nhấn nút **Thiết lập** trong mục **Cấu hình mật khẩu**.

Việc này sẽ mở ra thẻ **Authentication Agent** trong cửa sổ **Thiết lập mật khẩu mã hóa**.

8. Chọn hộp kiểm **Sử dụng công nghệ Single Sign-On (SSO)**.
9. Nhấn **OK**.
10. Để lưu thay đổi của bạn, trong cửa sổ **Thuộc tính: <Tên chính sách>**, nhấn **OK**.
11. Áp dụng chính sách.

    Xem *Hướng dẫn dành cho Quản trị viên Kaspersky Security Center* để biết chi tiết về việc áp dụng các chính sách Kaspersky Security Center.

Cân nhắc đặc biệt đối với mã hóa tập tin

Khi sử dụng chức năng mã hóa tập tin, hãy nhớ các điều sau:

- Chính sách của Kaspersky Security Center với thiết lập sẵn để mã hóa ổ đĩa di động được tạo cho một nhóm các máy tính được quản lý cụ thể. Do đó, kết quả của ứng dụng chính sách mã hóa / giải mã tập tin trên ổ đĩa di động phụ thuộc vào máy tính mà ổ đĩa di động đó được kết nối.
- Kaspersky Endpoint Security không mã hóa / giải mã các tập tin có trạng thái chỉ đọc được lưu trữ trên ổ đĩa di động.
- Kaspersky Endpoint Security sẽ chỉ mã hóa / giải mã các tập tin trong các thư mục được xác định trước cho hồ sơ người dùng cục bộ của hệ điều hành. Kaspersky Endpoint Security không mã hóa / giải mã các tập tin trong các thư mục được xác định trước cho hồ sơ người dùng chuyển vùng, hồ sơ người dùng bắt buộc, hồ sơ người dùng tạm thời và các thư mục được tái điều hướng. Danh sách các thư mục tiêu chuẩn được khuyến nghị bởi Kaspersky cho việc mã hóa bao gồm các thư mục sau:
  - My Documents
  - Favorites
  - Cookies
  - Desktop
  - Các tập tin trong thư mục Temporary Internet Explorer
  - Các tập tin tạm thời
  - Các tập tin Outlook
- Kaspersky Endpoint Security không thực hiện mã hóa các tập tin và thư mục nếu điều đó có thể làm hư hỏng hệ điều hành và các ứng dụng được cài đặt. Ví dụ, các tập tin và thư mục sau với tất cả các thư mục bên trong đều có tên trong danh sách loại trừ mã hóa:
  - %WINDIR%.
  - %PROGRAMFILES%, %PROGRAMFILES(X86)%.
  - Các tập tin registry của Windows.

Danh sách loại trừ mã hóa không thể được xem hoặc sửa. Trong khi các tập tin và thư mục trong danh sách loại trừ mã hóa có thể được thêm vào danh sách mã hóa, chúng không thể được mã hóa trong tác vụ mã hóa tập tin và thư mục.

- Các loại thiết bị sau được hỗ trợ làm ổ đĩa di động:
  - Dữ liệu đa phương tiện được kết nối qua cổng USB
  - ổ cứng được kết nối qua các bus USB và FireWire
  - Ổ SSD được kết nối qua các cổng USB và FireWire

Mã hóa các tập tin trên ổ đĩa cục bộ của máy tính

Tính năng mã hóa tập tin trên ổ đĩa của máy tính cục bộ có thể được sử dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Microsoft Windows cho máy trạm. Tính năng mã hóa tập tin trên ổ đĩa của máy tính cục bộ không thể được sử dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Microsoft Windows cho máy chủ tập tin.

Mục này chứa thông tin về việc mã hóa các tập tin trên ổ đĩa của máy tính cục bộ, và cung cấp chỉ dẫn về cách để thiết lập và thực hiện tác vụ mã hóa tập tin trên các ổ đĩa máy tính cục bộ sử dụng Kaspersky Endpoint Security và tiện ích Bảng điều khiển Kaspersky Endpoint Security.

Mã hóa các tập tin trên ổ đĩa cục bộ của máy tính

Để mã hóa các tập tin trên ổ đĩa cục bộ:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, mở thư mục với tên của nhóm quản trị mà bạn muốn thiết lập việc mã hóa các tập tin trên ổ đĩa cục bộ.
3. Trong không gian làm việc, chọn thẻ **Chính sách**.
4. Chọn chính sách cần thiết.
5. Mở cửa sổ **Thuộc tính: <Tên chính sách>** sử dụng một trong những phương pháp sau đây:
   - Trong menu ngữ cảnh của chính sách, chọn **Thuộc tính**.
   - Nhấn vào liên kết **Thiết lập chính sách** được đặt ở phần bên phải của không gian làm việc của Bảng điều khiển Quản trị.
6. Trong mục **Mã hóa dữ liệu**, chọn mục con **Mã hóa các tập tin và các thư mục**.
7. Ở phần bên phải của cửa sổ, chọn thẻ **Mã hóa**.
8. Trong danh sách thả xuống **Chế độ mã hóa**, chọn mục **Quy tắc mặc định**.
9. Trên thẻ **Mã hóa**, nhấn nút **Thêm**, và trong danh sách thả xuống chọn một trong các đề mục sau:

a. Chọn mục **Các thư mục được xác định trước** để thêm tập tin từ các thư mục của hồ sơ người dùng cục bộ theo khuyến nghị của các chuyên gia Kaspersky vào quy tắc mã hóa.

   Cửa sổ **Chọn các thư mục được xác định trước** sẽ được mở ra.

b. Chọn đề mục **Lọc tùy chỉnh** để thêm một đường dẫn thư mục được nhập thủ công vào quy tắc mã hóa.

   Cửa sổ **Thêm thư mục tùy chỉnh** sẽ được mở ra.

c. Chọn đề mục **Các tập tin có phần mở rộng** để thêm các phần mở rộng tập tin vào quy tắc mã hóa. Kaspersky Endpoint Security sẽ mã hóa các tập tin với phần mở rộng được quy định trên tất cả các ổ đĩa cục bộ của máy tính.

   Cửa sổ **Thêm / chỉnh sửa danh sách các phần mở rộng tập tin** sẽ được mở ra.

d. Chọn đề mục **Các tập tin có phần mở rộng theo nhóm** để thêm các nhóm phần mở rộng tập tin vào quy tắc mã hóa. Kaspersky Endpoint Security sẽ mã hóa các tập tin với phần mở rộng được liệt kê trong nhóm phần mở rộng này trên tất cả các ổ đĩa cục bộ của máy tính.

   Cửa sổ **Lựa chọn nhóm của phần mở rộng tập tin** sẽ được mở ra.

10. Để lưu thay đổi của bạn, trong cửa sổ **Thuộc tính: <Tên chính sách>**, nhấn **OK**.

11. Áp dụng chính sách.

    Xem *Hướng dẫn dành cho Quản trị viên Kaspersky Security Center* để biết chi tiết về việc áp dụng các chính sách Kaspersky Security Center.

Ngay khi chính sách này được áp dụng, Kaspersky Endpoint Security sẽ mã hóa các tập tin được bao gồm trong quy tắc mã hóa và không được bao gồm trong quy tắc giải mã.

Nếu tập tin này đã được thêm vào quy tắc mã hóa và quy tắc giải mã, Kaspersky Endpoint Security sẽ không mã hóa tập tin này nếu nó chưa được mã hóa, và giải mã tập tin này nếu nó đã được mã hóa.

Kaspersky Endpoint Security sẽ mã hóa các tập tin chưa được mã hóa nếu thuộc tính của chúng (đường dẫn tập tin / tên tập tin / phần mở rộng tập tin) vẫn đáp ứng được tiêu chí của quy tắc mã hóa sau khi được sửa đổi.

Kaspersky Endpoint Security sẽ hoãn việc mã hóa các tập tin đang mở cho đến khi chúng đã được đóng.

Khi người dùng tạo một tập tin mới có các thuộc tính đáp ứng tiêu chí của quy tắc mã hóa, Kaspersky Endpoint Security sẽ mã hóa tập tin này ngay khi nó được mở ra.

Nếu bạn di chuyển một tập tin được mã hóa đến một thư mục khác trên ổ đĩa cục bộ, tập tin đó vẫn sẽ được mã hóa bất kể thư mục này có được bao gồm trong quy tắc mã hóa hay không.

Tạo quy tắc truy cập tập tin được mã hóa cho ứng dụng

Để tạo quy tắc truy cập tập tin được mã hóa cho ứng dụng:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.

2. Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, mở thư mục với tên của nhóm quản trị mà bạn muốn thiết lập quy tắc truy cập tập tin được mã hóa cho ứng dụng.

3. Trong không gian làm việc, chọn thẻ **Chính sách**.

4. Chọn chính sách cần thiết.

5. Mở cửa sổ **Thuộc tính: <Tên chính sách>** sử dụng một trong những phương pháp sau đây:

   - Trong menu ngữ cảnh của chính sách, chọn **Thuộc tính**.
   - Nhấn vào liên kết **Thiết lập chính sách** được đặt ở phần bên phải của không gian làm việc của Bảng điều khiển Quản trị.

6. Trong mục **Mã hóa dữ liệu**, chọn mục con **Mã hóa các tập tin và các thư mục**.

7. Trong danh sách thả xuống **Chế độ mã hóa**, chọn mục **Quy tắc mặc định**.

   Quy tắc truy cập sẽ chỉ được áp dụng trong chế độ **Quy tắc mặc định**. Sau khi đã áp dụng quy tắc truy cập trong chế độ **Quy tắc mặc định**, nếu bạn chuyển sang chế độ **Giữ lại không thay đổi**, Kaspersky Endpoint Security sẽ bỏ qua tất cả các quy tắc truy cập. Mọi ứng dụng sẽ có thể truy cập tất cả các tập tin được mã hóa.

8. Ở phần bên phải của cửa sổ, chọn thẻ **Quy tắc cho ứng dụng**.

9. Nếu bạn muốn chỉ chọn ứng dụng từ danh sách Kaspersky Security Center, nhấn nút **Thêm** và trong danh sách thả xuống chọn mục **Các ứng dụng từ danh sách của Kaspersky Security Center**.

   Cửa sổ **Thêm các ứng dụng vào danh sách Kaspersky Security Center** sẽ được mở ra.

   Làm các bước sau:

   a. Quy định bộ lọc để rút ngắn danh sách ứng dụng trong bảng. Để làm điều này, nhập giá trị của các tham số **Ứng dụng**, **Nhà cung cấp**, và **Thời gian thêm vào**, và tất cả các hộp kiểm từ mục **Nhóm**.

   b. Nhấn vào nút **Làm mới**.

      Bảng này liệt kê các ứng dụng khớp với bộ lọc được áp dụng.

   c. Trong cột **Ứng dụng**, chọn các hộp kiểm đối diện ứng dụng mà bạn muốn tạo quy tắc truy cập tập tin được mã hóa cho chúng.

   d. Trong danh sách thả xuống **Quy tắc cho ứng dụng**, chọn quy tắc xác định quyền truy cập của ứng dụng đến các tập tin được mã hóa.

   e. Trong danh sách thả xuống **Hành động cho ứng dụng đã được chọn trước đó**, chọn hành động được thực thi bởi Kaspersky Endpoint Security đối với các quy tắc truy cập tập tin được mã hóa đã được tạo từ trước cho các ứng dụng này.

   f. Nhấn **OK**.

   Chi tiết của quy tắc truy cập tập tin được mã hóa cho các ứng dụng sẽ được hiển thị trong bảng trên thẻ **Quy tắc cho ứng dụng**.

10. Nếu bạn muốn chọn thủ công các ứng dụng, hãy nhấn nút **Thêm**, và trong danh sách thả xuống chọn mục **Các ứng dụng tùy chỉnh**.

    Cửa sổ **Thêm / chỉnh sửa tên của các tập tin thực thi ứng dụng** sẽ được mở ra.

    Làm các bước sau:

    a. Trong trường nhập liệu, nhập tên hoặc danh sách tên của các tập tin thực thi của các ứng dụng, bao gồm phần mở rộng của chúng.

Bạn cũng có thể bổ sung tên của các tập tin thực thi của các ứng dụng từ danh sách của Kaspersky Security Center bằng cách nhấn nút **Thêm từ danh sách Kaspersky Security Center**.

b. Nếu cần thiết, trong trường **Mô tả**, nhập mô tả cho danh sách ứng dụng này.

c. Trong danh sách thả xuống **Quy tắc cho ứng dụng**, chọn quy tắc xác định quyền truy cập của ứng dụng đến các tập tin được mã hóa.

d. Nhấn **OK**.

Chi tiết của quy tắc truy cập tập tin được mã hóa cho các ứng dụng sẽ được hiển thị trong bảng trên thẻ **Quy tắc cho ứng dụng**.

11. Nhấn **OK** để lưu thay đổi.

Mã hóa những tập tin được tạo hoặc sửa đổi bởi những ứng dụng cụ thể

Bạn có thể tạo một quy tắc mà theo đó Kaspersky Endpoint Security sẽ mã hóa tất cả các tập tin được tạo hoặc được sửa đổi bởi các ứng dụng được quy định trong quy tắc này.

Các tập tin được tạo hoặc sửa đổi bởi các ứng dụng được quy định trước khi quy tắc mã hóa được áp dụng sẽ không được mã hóa.

Để thiết lập việc mã hóa của những tập tin được tạo hoặc sửa đổi bởi các ứng dụng cụ thể:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, mở thư mục với tên của nhóm quản trị mà bạn muốn thiết lập việc mã hóa của những tập tin được tạo bởi các ứng dụng cụ thể.
3. Trong không gian làm việc, chọn thẻ **Chính sách**.
4. Chọn chính sách cần thiết.
5. Mở cửa sổ **Thuộc tính: <Tên chính sách>** sử dụng một trong những phương pháp sau đây:
   - Trong menu ngữ cảnh của chính sách, chọn **Thuộc tính**.
   - Nhấn vào liên kết **Thiết lập chính sách** được đặt ở phần bên phải của không gian làm việc của Bảng điều khiển Quản trị.
6. Trong mục **Mã hóa dữ liệu**, chọn mục con **Mã hóa các tập tin và các thư mục**.
7. Trong danh sách thả xuống **Chế độ mã hóa**, chọn mục **Quy tắc mặc định**.

Quy tắc mã hóa sẽ chỉ được áp dụng trong chế độ **Quy tắc mặc định**. Sau khi đã áp dụng quy tắc mã hóa trong chế độ **Quy tắc mặc định**, nếu bạn chuyển sang chế độ **Giữ lại không thay đổi**, Kaspersky Endpoint Security sẽ bỏ qua tất cả các quy tắc mã hóa. Các tập tin đã được mã hóa từ trước vẫn sẽ duy trì tình trạng mã hóa.

8. Ở phần bên phải của cửa sổ, chọn thẻ **Quy tắc cho ứng dụng**.

9. Nếu bạn muốn chỉ chọn ứng dụng từ danh sách Kaspersky Security Center, nhấn nút **Thêm** và trong danh sách thả xuống chọn mục **Các ứng dụng từ danh sách của Kaspersky Security Center**.

   Cửa sổ **Thêm các ứng dụng vào danh sách Kaspersky Security Center** sẽ được mở ra.

   Làm các bước sau:

   a. Quy định bộ lọc để rút ngắn danh sách ứng dụng trong bảng. Để làm điều này, nhập giá trị của các tham số **Ứng dụng**, **Nhà cung cấp**, và **Thời gian thêm vào**, và tất cả các hộp kiểm từ mục **Nhóm**.

   b. Nhấn vào nút **Làm mới**.

      Bảng này liệt kê các ứng dụng khớp với bộ lọc được áp dụng.

   c. Trong cột **Ứng dụng**, chọn hộp kiểm đối diện các ứng dụng mà những tập tin được tạo của chúng sẽ cần được mã hóa.

   d. Trong danh sách thả xuống **Quy tắc cho ứng dụng**, chọn **Mã hóa tất cả các tập tin được tạo**.

   e. Trong danh sách thả xuống **Hành động cho ứng dụng đã được chọn trước đó**, chọn hành động được thực thi bởi Kaspersky Endpoint Security đối với các quy tắc mã hóa tập tin đã được tạo từ trước cho các ứng dụng này.

   f. Nhấn **OK**.

   Thông tin về quy tắc mã hóa cho các tập tin được tạo hoặc được sửa đổi bởi các ứng dụng được chọn sẽ xuất hiện trong bảng trên thẻ **Quy tắc cho ứng dụng**.

10. Nếu bạn muốn chọn thủ công các ứng dụng, hãy nhấn nút **Thêm**, và trong danh sách thả xuống chọn mục **Các ứng dụng tùy chỉnh**.

    Cửa sổ **Thêm / chỉnh sửa tên của các tập tin thực thi ứng dụng** sẽ được mở ra.

    Làm các bước sau:

    a. Trong trường nhập liệu, nhập tên hoặc danh sách tên của các tập tin thực thi của các ứng dụng, bao gồm phần mở rộng của chúng.

       Bạn cũng có thể bổ sung tên của các tập tin thực thi của các ứng dụng từ danh sách của Kaspersky Security Center bằng cách nhấn nút **Thêm từ danh sách Kaspersky Security Center**.

    b. Nếu cần thiết, trong trường **Mô tả**, nhập mô tả cho danh sách ứng dụng này.

    c. Trong danh sách thả xuống **Quy tắc cho ứng dụng**, chọn **Mã hóa tất cả các tập tin được tạo**.

    d. Nhấn **OK**.

    Thông tin về quy tắc mã hóa cho các tập tin được tạo hoặc được sửa đổi bởi các ứng dụng được chọn sẽ xuất hiện trong bảng trên thẻ **Quy tắc cho ứng dụng**.

11. Nhấn **OK** để lưu thay đổi.

Tạo một quy tắc giải mã

Để tạo một quy tắc giải mã:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, mở thư mục với tên của nhóm quản trị mà bạn muốn tạo một danh sách các tập tin được giải mã.
3. Trong không gian làm việc, chọn thẻ **Chính sách**.
4. Chọn chính sách cần thiết.
5. Mở cửa sổ **Thuộc tính: <Tên chính sách>** sử dụng một trong những phương pháp sau đây:
   - Trong menu ngữ cảnh của chính sách, chọn **Thuộc tính**.
   - Nhấn vào liên kết **Thiết lập chính sách** được đặt ở phần bên phải của không gian làm việc của Bảng điều khiển Quản trị.
6. Trong mục **Mã hóa dữ liệu**, chọn mục con **Mã hóa các tập tin và các thư mục**.
7. Ở phần bên phải của cửa sổ, chọn thẻ **Giải mã**.
8. Trong danh sách thả xuống **Chế độ mã hóa**, chọn mục **Quy tắc mặc định**.
9. Trên thẻ **Giải mã**, nhấn nút **Thêm**, và trong danh sách thả xuống chọn một trong các đề mục sau:
   a. Chọn mục **Các thư mục được xác định trước** để thêm tập tin từ các thư mục của hồ sơ người dùng cục bộ theo khuyến nghị của các chuyên gia Kaspersky vào quy tắc giải mã.

      Cửa sổ **Chọn các thư mục được xác định trước** sẽ được mở ra.

   b. Chọn đề mục **Lọc tùy chỉnh** để thêm một đường dẫn thư mục được nhập thủ công vào quy tắc giải mã.

      Cửa sổ **Thêm thư mục tùy chỉnh** sẽ được mở ra.

   c. Chọn đề mục **Các tập tin có phần mở rộng** để thêm các phần mở rộng tập tin vào quy tắc giải mã. Kaspersky Endpoint Security sẽ không mã hóa các tập tin với phần mở rộng được quy định trên tất cả các ổ đĩa cục bộ của máy tính.

      Cửa sổ **Thêm / chỉnh sửa danh sách các phần mở rộng tập tin** sẽ được mở ra.

   d. Chọn đề mục **Các tập tin có phần mở rộng theo nhóm** để thêm các nhóm phần mở rộng tập tin vào quy tắc giải mã. Kaspersky Endpoint Security sẽ không mã hóa các tập tin với phần mở rộng được liệt kê trong nhóm phần mở rộng này trên tất cả các ổ đĩa cục bộ của máy tính.

      Cửa sổ **Lựa chọn nhóm của phần mở rộng tập tin** sẽ được mở ra.
10. Để lưu thay đổi của bạn, trong cửa sổ **Thuộc tính: <Tên chính sách>**, nhấn **OK**.
11. Áp dụng chính sách.

    Xem *Hướng dẫn dành cho Quản trị viên Kaspersky Security Center* để biết chi tiết về việc áp dụng các chính sách Kaspersky Security Center.

Nếu tập tin này đã được thêm vào quy tắc mã hóa và quy tắc giải mã, Kaspersky Endpoint Security sẽ không mã hóa tập tin này nếu nó chưa được mã hóa, và giải mã tập tin này nếu nó đã được mã hóa.

Giải mã các tập tin trên ổ đĩa cục bộ trên máy tính

Để giải mã các tập tin trên ổ đĩa cục bộ:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, mở thư mục với tên của nhóm quản trị mà bạn muốn thiết lập việc giải mã các tập tin trên ổ đĩa cục bộ.
3. Trong không gian làm việc, chọn thẻ **Chính sách**.
4. Chọn chính sách cần thiết.
5. Mở cửa sổ **Thuộc tính: <Tên chính sách>** sử dụng một trong những phương pháp sau đây:
   - Trong menu ngữ cảnh của chính sách, chọn **Thuộc tính**.
   - Nhấn vào liên kết **Thiết lập chính sách** được đặt ở phần bên phải của không gian làm việc của Bảng điều khiển Quản trị.
6. Trong mục **Mã hóa dữ liệu**, chọn mục con **Mã hóa các tập tin và các thư mục**.
7. Ở phần bên phải của cửa sổ, chọn thẻ **Mã hóa**.
8. Xóa các tập tin và thư mục mà bạn muốn giải mã khỏi danh sách mã hóa. Để làm việc này, chọn các tập tin và chọn mục **Xóa quy tắc và giải mã tập tin** trong menu ngữ cảnh của nút **Gỡ bỏ**.

   Bạn có thể xóa vài tập tin một lúc từ danh sách mã hóa. Để làm việc này, trong khi giữ phím **CTRL**, chọn các tập tin mà bạn cần bằng cách nhấn trái chuột lên chúng và chọn mục **Xóa quy tắc và giải mã tập tin** trong menu ngữ cảnh của nút **Gỡ bỏ**.

   Các tập tin và thư mục được xóa khỏi danh sách mã hóa sẽ tự động được thêm vào danh sách giải mã.
9. Tạo một danh sách giải mã tập tin.
10. Để lưu thay đổi của bạn, trong cửa sổ **Thuộc tính: <Tên chính sách>**, nhấn **OK**.
11. Áp dụng chính sách.

Xem *Hướng dẫn dành cho Quản trị viên Kaspersky Security Center* để biết chi tiết về việc áp dụng các chính sách Kaspersky Security Center.

Ngay khi chính sách này được áp dụng, Kaspersky Endpoint Security sẽ giải mã các tập tin được mã hóa được thêm vào danh sách giải mã.

Kaspersky Endpoint Security sẽ giải mã các tập tin được mã hóa nếu tham số của chúng (đường dẫn tập tin / tên tập tin / phần mở rộng tập tin) được thay đổi để khớp với tham số của các đối tượng được thêm vào danh sách giải mã.

Kaspersky Endpoint Security sẽ hoãn việc giải mã các tập tin đang mở cho đến khi chúng đã được đóng.

Tạo các gói được mã hóa

Kaspersky Endpoint Security sẽ không nén tập tin khi nó tạo một gói được mã hóa.

Để tạo một gói được mã hóa:

1. Tren máy tính có cài đặt Kaspersky Endpoint Security và có bật chức năng mã hóa, sử dụng bất kỳ trình quản lý tập tin nào để chọn các tập tin và thư mục mà bạn muốn thêm vào một gói được mã hóa. Nhấn phải chuột để mở menu ngữ cảnh.

2. Trong menu ngữ cảnh, chọn **Thêm gói mã hóa**.

   Hộp thoại tiêu chuẩn **Chọn đường dẫn để lưu gói phần mềm được mã hóa** của Microsoft Windows sẽ được mở ra.

3. Trong hộp thoại tiêu chuẩn **Chọn đường dẫn để lưu gói phần mềm được mã hóa** của Microsoft Windows, chọn đích để lưu gói được mã hóa lên ổ đĩa di động. Nhấp vào nút **Lưu**.

   Cửa sổ **Thêm gói mã hóa** sẽ được mở ra.

4. Trong cửa sổ **Thêm gói mã hóa**, nhập và xác nhận mật khẩu.

5. Nhấn nút **Tạo**.

   Tiến trình tạo gói được mã hóa sẽ được bắt đầu. Khi tiến trình này kết thúc, một gói mã hóa được bảo vệ bởi mật khẩu có thể tự giải nén sẽ được tạo trong thư mục đích được chọn trên ổ đĩa di động.

Nếu bạn hủy bỏ việc tạo một gói được mã hóa, Kaspersky Endpoint Security sẽ thực hiện hoạt động sau:

1. Chấm dứt tiến trình sao chép tập tin đến gói và chấm dứt mọi hoạt động mã hóa gói đang diễn ra nếu có.

2. Xóa tất cả các tập tin tạm thời đã được tạo trong tiến trình tạo và mã hóa một gói tin và cả gói được mã hóa đó.

3. Thông báo với người dùng rằng tiến trình tạo gói được mã hóa đã bị buộc chấm dứt.

Giải nén các gói được mã hóa

Để giải nén một gói được mã hóa:

1. Trong bất kỳ trình quản lý tập tin nào, chọn một gói được mã hóa. Nhấn để bắt đầu Trình hướng dẫn Giải nén.

   Cửa sổ **Nhập mật khẩu** sẽ được mở ra.

2. Nhập mật khẩu bảo vệ gói được mã hóa.

3. Trong cửa sổ **Nhập mật khẩu**, nhấn **OK**.

   Nếu mật khẩu được nhập thành công, hộp thoại **Duyệt** tiêu chuẩn của Microsoft Windows sẽ được mở ra.

4. Trong hộp thoại **Duyệt** tiêu chuẩn của Microsoft Windows, chọn thư mục đích để giải nén gói được mã hóa và nhấn **OK**.

   Tiến trình giải nén gói được mã hóa đến thư mục đích sẽ được bắt đầu.

Nếu trước đó gói được mã hóa đã được giải nén đến thư mục đích được quy định, các tập tin hiện có trong thư mục sẽ bị ghi đè với tập tin từ gói được mã hóa.

Nếu bạn hủy bỏ việc giải nén một gói được mã hóa, Kaspersky Endpoint Security sẽ thực hiện hoạt động sau:

1. Dừng tiến trình giải mã gói và chấm dứt mọi hoạt động sao chép tập tin từ gói được mã hóa nếu hoạt động đó đang diễn ra.
2. Xóa tất cả các tập tin tạm thời được tạo trong quá trình giải mã và giải nén gói được mã hóa, cũng như tất cả các tập tin đã được sao chép từ gói được mã hóa đến thư mục đích.
3. Thông báo với người dùng rằng tiến trình giải nén gói được mã hóa đã bị buộc chấm dứt.

Mã hóa ổ đĩa di động

Tính năng mã hóa các ổ đĩa di động có thể được sử dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Microsoft Windows cho máy trạm. Tính năng mã hóa các ổ đĩa di động không thể được sử dụng nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Microsoft Windows cho máy chủ tập tin.

Mục này chứa thông tin về việc mã hóa các ổ đĩa di động và chỉ dẫn về cách để thiết lập và thực hiện tác vụ mã hóa các ổ đĩa di động sử dụng Kaspersky Endpoint Security và tiện ích quản trị Kaspersky Endpoint Security.

Bắt đầu mã hóa ổ đĩa di động

Để mã hóa ổ đĩa di động:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, mở thư mục với tên của nhóm quản trị mà bạn muốn thiết lập việc mã hóa các ổ đĩa di động.
3. Trong không gian làm việc, chọn thẻ **Chính sách**.
4. Chọn chính sách cần thiết.
5. Mở cửa sổ **Thuộc tính: <Tên chính sách>** sử dụng một trong những phương pháp sau đây:
   - Trong menu ngữ cảnh của chính sách, chọn **Thuộc tính**.
   - Nhấn vào liên kết **Thiết lập chính sách** được đặt ở phần bên phải của không gian làm việc của Bảng điều khiển Quản trị.
6. Trong mục **Mã hóa dữ liệu**, chọn mục con **Mã hóa ổ đĩa di động**.

7. Trong danh sách thả xuống **Chế độ mã hóa**, chọn hành động mặc định được thực hiện bởi Kaspersky Endpoint Security trên tất cả các ổ đĩa di động được kết nối đến máy tính trong nhóm quản trị được chọn:

   - **Mã hóa toàn bộ ổ đĩa di động**. Nếu mục này được chọn, khi áp dụng chính sách của Kaspersky Security Center với cấu hình mã hóa được quy định cho ổ đĩa di động, Kaspersky Endpoint Security sẽ mã hóa nội dung của ổ đĩa di động theo từng khu vực. Kết quả là, ứng dụng sẽ không chỉ mã hóa các tập tin được lưu trữ trên ổ đĩa di động, mà còn hệ thống tập tin của các ổ đĩa di động, bao gồm tên tập tin và cấu trúc thư mục. Kaspersky Endpoint Security sẽ không tái mã hóa các ổ đĩa di động đã được mã hóa từ trước.

     Tình huống mã hóa này được cho phép bởi chức năng mã hóa ổ cứng của Kaspersky Endpoint Security.

   - **Mã hóa tất cả các tập tin**. Nếu mục này được chọn, khi áp dụng chính sách Kaspersky Security Center với cấu hình mã hóa được quy định cho các ổ đĩa di động, Kaspersky Endpoint Security sẽ mã hóa tất cả các tập tin được lưu trữ trên ổ đĩa di động. Kaspersky Endpoint Security sẽ không mã hóa lại các tập tin đã được mã hóa. Ứng dụng sẽ không mã hóa hệ thống tập tin của ổ đĩa di động, bao gồm tên của các tập tin và cấu trúc thư mục được mã hóa.

   - **Chỉ mã hóa các tập tin mới**. Nếu mục này được chọn, khi áp dụng chính sách của Kaspersky Security Center với cấu hình mã hóa được quy định cho ổ đĩa di động, Kaspersky Endpoint Security sẽ chỉ mã hóa các tập tin đã được thêm vào ổ đĩa di động hoặc được lưu trữ trên ổ đĩa di động và đã được thay đổi sau khi được áp dụng chính sách Kaspersky Security Center từ lần trước.

   - **Giải mã toàn bộ ổ đĩa di động**. Nếu mục này được chọn, khi áp dụng chính sách của Kaspersky Security Center với cấu hình mã hóa được quy định cho ổ đĩa di động, Kaspersky Endpoint Security sẽ giải mã tất cả các tập tin được mã hóa trên ổ đĩa di động cũng như các hệ thống tập tin của ổ đĩa di động nếu trước đó chúng đã được mã hóa.

     Tình huống mã hóa này có thể xảy ra bởi chức năng mã hóa tập tin và mã hóa ổ cứng của Kaspersky Endpoint Security.

   - **Giữ lại không thay đổi**. Nếu mục này được chọn, khi áp dụng chính sách của Kaspersky Security Center với cấu hình mã hóa được quy định cho ổ đĩa di động, Kaspersky Endpoint Security sẽ không mã hóa hoặc giải mã các tập tin trên ổ đĩa di động.

8. Tạo quy tắc mã hóa cho các tập tin trên ổ đĩa di động có nội dung mà bạn muốn mã hóa.

9. Áp dụng chính sách.

Xem *Hướng dẫn dành cho Quản trị viên Kaspersky Security Center* để biết chi tiết về việc áp dụng các chính sách Kaspersky Security Center.

Ngay khi chính sách được áp dụng, khi người dùng kết nối một ổ đĩa di động hoặc nếu ổ đĩa di động đã được kết nối, Kaspersky Endpoint Security sẽ thông báo với người dùng rằng ổ đĩa di động này tuân thủ một quy tắc mã hóa mà ở đó dữ liệu được lưu trữ trên ổ đĩa di động sẽ được mã hóa.

Nếu quy tắc *Không thay đổi* được quy định cho việc mã hóa dữ liệu trên một ổ đĩa di động, ứng dụng sẽ không hiển thị bất kỳ thông báo nào cho người dùng.

Ứng dụng sẽ cảnh báo người dùng rằng tiến trình mã hóa sẽ mất một khoảng thời gian.

Ứng dụng sẽ nhắc người dùng xác nhận hoạt động mã hóa và thực hiện các hành động sau:

- Mã hóa dữ liệu theo cấu hình chính sách, nếu người dùng đồng ý với việc mã hóa.
- Để nguyên, không mã hóa dữ liệu nếu người dùng từ chối mã hóa, và hạn chế truy cập đến các tập tin trên ổ đĩa di động ở mức chỉ đọc.
- Để nguyên, không mã hóa dữ liệu nếu người dùng bỏ qua lời nhắc mã hóa, hạn chế truy cập đến các tập tin trên ổ đĩa di động ở mức chỉ đọc, và nhắc người dùng xác nhận lại việc mã hóa dữ liệu khi chính sách Kaspersky Security Center được áp dụng ở lần tiếp theo, hoặc khi một ổ đĩa di động được kết nối.

Chính sách của Kaspersky Security Center với thiết lập sẵn để mã hóa dữ liệu trên ổ đĩa di động được tạo cho một nhóm các máy tính được quản lý cụ thể. Do đó, kết quả mã hóa dữ liệu trên ổ đĩa di động phụ thuộc vào máy tính mà ổ đĩa di động đó được kết nối.

Nếu người dùng tiến hành gỡ bỏ an toàn một ổ đĩa di động trong quá trình mã hóa dữ liệu, Kaspersky Endpoint Security sẽ ngắt tiến trình mã hóa dữ liệu và cho phép việc gỡ bỏ ổ đĩa di động trước khi tiến trình mã hóa được kết thúc.

Nếu quá trình mã hóa ổ đĩa di động thất bại, hãy xem báo cáo **Mã hóa dữ liệu** trong giao diện Kaspersky Endpoint Security. Một ứng dụng khác có thể chặn quyền truy cập các tập tin. Trong trường hợp này, hãy thử rút ổ đĩa di động đó ra khỏi máy tính và thử kết nối lại.

Thêm một quy tắc mã hóa cho ổ đĩa di động

Để thêm một quy tắc mã hóa cho ổ đĩa di động:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, mở thư mục với tên của nhóm quản trị mà bạn muốn thêm các quy tắc mã hóa ổ đĩa di động.
3. Trong không gian làm việc, chọn thẻ **Chính sách**.
4. Chọn chính sách cần thiết.
5. Mở cửa sổ **Thuộc tính: <Tên chính sách>** sử dụng một trong những phương pháp sau đây:
   - Trong menu ngữ cảnh của chính sách, chọn **Thuộc tính**.
   - Nhấn vào liên kết **Thiết lập chính sách** được đặt ở phần bên phải của không gian làm việc của Bảng điều khiển Quản trị.
6. Trong mục **Mã hóa dữ liệu**, chọn mục con **Mã hóa ổ đĩa di động**.
7. Nhấn trái chuột lên nút **Thêm**, và trong danh sách thả xuống chọn một trong các đề mục sau:
   - Nếu bạn muốn thêm quy tắc mã hóa cho các ổ đĩa di động nằm trong danh sách các thiết bị được tin tưởng của thành phần Kiểm soát Thiết bị, chọn **Từ danh sách các thiết bị tin tưởng cùa chính sách này**.

     Cửa sổ **Thêm thiết bị vào danh sách các thiết bị tin tưởng** sẽ được mở ra.

- Nếu bạn muốn thêm quy tắc mã hóa cho các ổ đĩa di động nằm trong danh sách Kaspersky Security Center, chọn **Từ danh sách thiết bị của Kaspersky Security Center**.

  Cửa sổ **Thêm các thiết bị vào danh sách Kaspersky Security Center** sẽ được mở ra.

8. Nếu bạn đã chọn **Từ danh sách thiết bị của Kaspersky Security Center** ở bước trước, hãy quy định bộ lọc để hiển thị các thiết bị trong bảng. Để làm điều này:

   a. Quy định giá trị của các tham số sau: **Hiển thị các thiết bị trong bảng được định nghĩa sau**, **Loại thiết bị**, **Tên**, **Máy tính**, và **Kaspersky Disk Encryption**.

   b. Nhấn vào nút **Làm mới**.

9. Trong cột **Loại thiết bị**, chọn hộp kiểm đối diện tên của các ổ đĩa di động mà bạn muốn tạo quy tắc mã hóa.

10. Trong danh sách thả xuống **Chế độ mã hóa cho thiết bị đã được chọn**, chọn hành động được thực hiện bởi Kaspersky Endpoint Security trên các tập tin được lưu trữ trên các ổ đĩa di động được chọn.

11. Chọn hộp kiểm **Chế độ lưu động** nếu bạn muốn Kaspersky Endpoint Security chuẩn bị các ổ đĩa di động trước khi mã hóa, để bạn có thể sử dụng các tập tin được mã hóa trên chúng trong chế độ lưu động.

    Chế độ lưu động cho phép bạn sử dụng các tập tin được mã hóa trên các ổ đĩa di động kết nối đến các máy tính không có chức năng mã hóa.

12. Chọn hộp kiểm **Chỉ mã hóa dung lượng ổ đĩa được sử dụng** nếu bạn muốn Kaspersky Endpoint Security chỉ mã hóa các vùng ổ đĩa có lưu trữ tập tin.

    Nếu bạn đang áp dụng mã hóa trên một ổ đĩa đang được sử dụng, bạn nên mã hóa toàn bộ ổ đĩa. Điều này đảm bảo mọi dữ liệu đều được bảo vệ - kể cả những dữ liệu đã bị xóa có thể vẫn chứa thông tin truy hồi được. Chức năng **Chỉ mã hóa dung lượng ổ đĩa được sử dụng** được khuyến nghị cho các ổ đĩa mới chưa được sử dụng trước đây.

    Nếu một thiết bị đã được mã hóa từ trước sử dụng chức năng **Chỉ mã hóa dung lượng ổ đĩa được sử dụng**, sau khi áp dụng một chính sách trong chế độ **Mã hóa toàn bộ ổ đĩa di động**, các khu vực không chứa tập tin vẫn sẽ không được mã hóa.

13. Trong danh sách thả xuống **Hành động cho thiết bị đã được chọn trước đó**, chọn hành động được thực thi bởi Kaspersky Endpoint Security theo các quy tắc mã hóa đã được quy định từ trước cho ổ đĩa di động:

    - Nếu bạn muốn quy tắc mã hóa đã được tạo từ trước cho ổ đĩa di động không được thay đổi, chọn **Bỏ qua**.

    - Nếu bạn muốn thay thế một quy tắc mã hóa đã được tạo từ trước cho một ổ đĩa di động với một quy tắc mới, chọn **Cập nhật**.

14. Nhấn **OK**.

    Các dòng chứa tham số của quy tắc mã hóa được tạo sẽ xuất hiện trong bảng **Quy tắc tùy chỉnh**.

15. Nhấn **OK** để lưu thay đổi.

Các quy tắc mã hóa ổ đĩa di động vừa được thêm sẽ được áp dụng cho các ổ đĩa di động kết nối đến bất kỳ máy tính nào được kiểm soát bởi chính sách đã thay đổi của Kaspersky Security Center.

Sửa một quy tắc mã hóa cho ổ đĩa di động

Để sửa một quy tắc mã hóa cho một ổ đĩa di động:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, mở thư mục với tên của nhóm quản trị mà bạn muốn sửa một quy tắc mã hóa ổ đĩa di động.
3. Trong không gian làm việc, chọn thẻ **Chính sách**.
4. Chọn chính sách cần thiết.
5. Mở cửa sổ **Thuộc tính: <Tên chính sách>** sử dụng một trong những phương pháp sau đây:
   - Trong menu ngữ cảnh của chính sách, chọn **Thuộc tính**.
   - Nhấn vào liên kết **Thiết lập chính sách** được đặt ở phần bên phải của không gian làm việc của Bảng điều khiển Quản trị.
6. Trong mục **Mã hóa dữ liệu**, chọn mục con **Mã hóa ổ đĩa di động**.
7. Trong danh sách các ổ đĩa di động đã được thiết lập quy tắc mã hóa, chọn một mục tương ứng với ổ đĩa di động mà bạn cần.
8. Nhấn vào nút **Thiết lập quy tắc** để sửa quy tắc mã hóa cho ổ đĩa di động được chọn.
   Menu ngữ cảnh của nút **Thiết lập quy tắc** sẽ được mở ra.
9. Trong menu ngữ cảnh của nút **Thiết lập quy tắc**, chọn hành động được thực hiện bởi Kaspersky Endpoint Security trên các tập tin được lưu trữ trên ổ đĩa di động được chọn.
10. Nhấn **OK** để lưu thay đổi.

Các quy tắc mã hóa ổ đĩa di động vừa được thay đổi sẽ được áp dụng cho các ổ đĩa di động kết nối đến bất kỳ máy tính nào được kiểm soát bởi chính sách đã thay đổi của Kaspersky Security Center.

Bật chế độ lưu động để truy cập các tập tin được mã hóa trên ổ đĩa di động

Để bật chế độ lưu động để truy cập các tập tin được mã hóa trên ổ đĩa di động:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, mở thư mục với tên của nhóm quản trị mà bạn muốn bật chế độ lưu động để truy cập các tập tin được mã hóa trên ổ đĩa di động.
3. Trong không gian làm việc, chọn thẻ **Chính sách**.
4. Chọn chính sách cần thiết.
5. Mở cửa sổ **Thuộc tính: <Tên chính sách>** sử dụng một trong những phương pháp sau đây:

- Trong menu ngữ cảnh của chính sách, chọn **Thuộc tính**.
- Nhấn vào liên kết **Thiết lập chính sách** được đặt ở phần bên phải của không gian làm việc của Bảng điều khiển Quản trị.

6. Trong mục **Mã hóa dữ liệu**, chọn mục con **Mã hóa ổ đĩa di động**.
7. Chọn hộp kiểm **Chế độ lưu động**.

   Chế độ lưu động có thể được sử dụng để mã hóa tất cả các tập tin, hoặc chỉ các tập tin mới.

8. Nhấn **OK**.
9. Áp dụng chính sách.

   Xem *Hướng dẫn dành cho Quản trị viên Kaspersky Security Center* để biết chi tiết về việc áp dụng các chính sách Kaspersky Security Center.

10. Kết nối ổ đĩa di động đến thiết bị được áp dụng chính sách Kaspersky Security Center.
11. Xác nhận thao tác mã hóa ổ đĩa di động.

    Thao tác này mở ra một cửa sổ trong đó bạn có thể tạo một mật khẩu cho Portable File Manager.

12. Nhập một mật khẩu đáp ứng được yêu cầu về độ bảo mật và xác nhận nó.
13. Nhấn **OK**.

    Kaspersky Endpoint Security sẽ mã hóa các tập tin trên một ổ đĩa di động theo các quy tắc mã hóa được quy định trong chính sách của Kaspersky Security Center. Portable File Manager được sử dụng để làm việc với các tập tin mã hóa cũng sẽ được ghi vào ổ đĩa di động.

Sau khi đã bật chế độ lưu động, bạn có thể truy cập các tập tin được mã hóa trên ổ đĩa di động được kết nối đến một máy tính không có chức năng mã hóa.

Giải mã ổ đĩa di động

Để giải mã ổ đĩa di động:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, mở thư mục với tên của nhóm quản trị mà bạn muốn thiết lập việc giải mã các ổ đĩa di động.
3. Trong không gian làm việc, chọn thẻ **Chính sách**.
4. Chọn chính sách cần thiết.
5. Mở cửa sổ **Thuộc tính: <Tên chính sách>** sử dụng một trong những phương pháp sau đây:
   - Trong menu ngữ cảnh của chính sách, chọn **Thuộc tính**.
   - Nhấn vào liên kết **Thiết lập chính sách** được đặt ở phần bên phải của không gian làm việc của Bảng điều khiển Quản trị.

6. Trong mục **Mã hóa dữ liệu**, chọn mục con **Mã hóa ổ đĩa di động**.

7. Nếu bạn muốn giải mã tất cả các tập tin được mã hóa trên ổ đĩa di động, trong danh sách thả xuống **Chế độ mã hóa**, chọn **Giải mã toàn bộ ổ đĩa di động**.

8. Để giải mã dữ liệu được lưu trữ trên các ổ đĩa di động riêng lẻ, hãy sửa quy tắc mã hóa cho các ổ đĩa di động có dữ liệu mà bạn muốn giải mã. Để làm điều này:

   a. Trong danh sách các ổ đĩa di động đã được thiết lập quy tắc mã hóa, chọn một mục tương ứng với ổ đĩa di động mà bạn cần.

   b. Nhấn vào nút **Thiết lập quy tắc** để sửa quy tắc mã hóa cho ổ đĩa di động được chọn.

   Menu ngữ cảnh của nút **Thiết lập quy tắc** sẽ được mở ra.

   c. Chọn mục **Giải mã tất cả các tập tin** trong menu ngữ cảnh của nút **Thiết lập quy tắc**.

9. Nhấn **OK** để lưu thay đổi.

10. Áp dụng chính sách.

Xem *Hướng dẫn dành cho Quản trị viên Kaspersky Security Center* để biết chi tiết về việc áp dụng các chính sách Kaspersky Security Center.

Sau khi chính sách đã được áp dụng, khi người dùng kết nối đến một ổ đĩa di động hoặc nếu ổ đĩa di động đã được kết nối, Kaspersky Endpoint Security sẽ thông báo với người dùng rằng ổ đĩa di động này tuân thủ một quy tắc mã hóa mà ở đó các tập tin được mã hóa trên ổ đĩa di động cũng như hệ thống tập tin của ổ đĩa di động (nếu nó được mã hóa) sẽ được giải mã. Ứng dụng sẽ cảnh báo người dùng rằng tiến trình giải mã sẽ mất một khoảng thời gian.

Chính sách của Kaspersky Security Center với thiết lập sẵn để mã hóa dữ liệu trên ổ đĩa di động được tạo cho một nhóm các máy tính được quản lý cụ thể. Do đó, kết quả giải mã dữ liệu trên ổ đĩa di động phụ thuộc vào máy tính mà ổ đĩa di động đó được kết nối.

Nếu người dùng tiến hành gỡ bỏ an toàn một ổ đĩa di động trong quá trình giải mã dữ liệu, Kaspersky Endpoint Security sẽ ngắt tiến trình giải mã dữ liệu và cho phép việc gỡ bỏ ổ đĩa di động trước khi hoạt động giải mã được kết thúc.

Nếu quá trình giải mã ổ đĩa di động thất bại, hãy xem báo cáo **Mã hóa dữ liệu** trong giao diện Kaspersky Endpoint Security. Một ứng dụng khác có thể chặn quyền truy cập các tập tin. Trong trường hợp này, hãy thử rút ổ đĩa di động đó ra khỏi máy tính và thử kết nối lại.

Mã hóa ổ cứng

Nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Microsoft Windows for Workstations, các công nghệ BitLocker Drive Encryption và Kaspersky Disk Encryption có thể được sử dụng để mã hóa. Nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Microsoft Windows cho Máy chủ Tập tin, chỉ công nghệ BitLocker Drive Encryption là có thể được sử dụng.

Mục này chứa thông tin về việc mã hóa các ổ cứng và chỉ dẫn về cách để thiết lập và thực hiện tác vụ mã hóa các ổ cứng sử dụng Kaspersky Endpoint Security và tiện ích Bảng điều khiển Kaspersky Endpoint Security.

Thông tin về mã hóa ổ cứng

Trước khi bắt đầu mã hóa ổ cứng, ứng dụng sẽ chạy một số kiểm tra để xác định rằng liệu thiết bị có thể được mã hóa hay không, điều này bao gồm kiểm tra ổ cứng hệ thống để phát hiện tính tương thích với Authentication Agent và các thành phần mã hóa BitLocker. Để kiểm tra tính tương thích, máy tính phải được khởi động lại. Sau khi máy tính đã được khởi động lại, ứng dụng sẽ tự động thực hiện tất cả các kiểm tra cần thiết. Nếu kiểm tra tính tương thích thành công, tác vụ mã hóa ổ cứng sẽ được bắt đầu sau khi hệ điều hành đã khởi động và ứng dụng đã được khởi chạy. Nếu ổ cứng hệ thống được phát hiện là không tương thích với Authentication Agent hoặc với các thành phần mã hóa BitLocker, máy tính phải được khởi động lại bằng cách nhấn nút cứng Khởi động lại. Kaspersky Endpoint Security sẽ ghi lại thông tin về tình trạng không tương thích. Dựa trên thông tin này, ứng dụng sẽ không bắt đầu mã hóa ổ cứng khi khởi động hệ điều hành. Thông tin về sự kiện này sẽ được ghi lại trong báo cáo của Kaspersky Security Center.

Nếu thiết lập phần cứng của máy tính đã thay đổi, thông tin về tình trạng không tương thích được ghi lại bởi ứng dụng trong lần kiểm tra trước nên được xóa để có thể kiểm tra lại ổ cứng hệ thống cho sự tương thích với Authentication Agent và các thành phần mã hóa BitLocker. Để làm điều này, trước khi mã hóa ổ cứng, nhập `avp pbatestreset` vào dòng lệnh. Nếu hệ điều hành không thể nạp sau khi ổ cứng hệ thống đã được xác định là tương thích với Authentication Agent, bạn phải xóa các đối tượng và dữ liệu còn sót lại sau hoạt động thử nghiệm của Authentication Agent bằng cách sử dụng Tiện ích Khôi phục và sau đó khởi động Kaspersky Endpoint Security và thực thi lệnh `avp pbatestreset` một lần nữa.

Sau khi quá trình mã hóa ổ cứng đã được bắt đầu, Kaspersky Endpoint Security sẽ mã hóa tất cả dữ liệu được ghi vào ổ cứng.

Nếu người dùng tắt hoặc khởi động lại máy tính trong quá trình giải mã ổ cứng, Authentication Agent sẽ được nạp trước lần khởi động hệ điều hành tiếp theo. Kaspersky Endpoint Security sẽ tiếp tục quá trình mã hóa ổ cứng sau khi xác thực thành công trong authentication agent và trong quá trình khởi động hệ điều hành.

Nếu hệ điều hành được chuyển sang chế độ ngủ đông khi ổ cứng đang được mã hóa, Authentication Agent sẽ được nạp khi hệ điều hành ra khỏi chế độ ngủ đông. Kaspersky Endpoint Security sẽ tiếp tục quá trình mã hóa ổ cứng sau khi xác thực thành công trong authentication agent và trong quá trình khởi động hệ điều hành.

Nếu hệ điều hành chuyển sang chế độ ngủ trong quá trình mã hóa ổ cứng, Kaspersky Endpoint Security sẽ tiếp tục mã hóa ổ cứng khi hệ điều hành ra khỏi chế độ ngủ mà không nạp Authentication Agent.

Việc xác thực người dùng trong Authentication Agent có thể được thực hiện bằng hai cách:

- Nhập tên và mật khẩu của tài khoản Authentication Agent được tạo bởi quản trị viên mạng LAN với các công cụ của Kaspersky Security Center.
- Nhập mật khẩu của một token hoặc thẻ thông minh được kết nối đến máy tính.

Authentication Agent hỗ trợ bố cục bàn phím cho các ngôn ngữ sau đây:

- Tiếng Anh (Vương Quốc Anh)
- Tiếng Anh (Mỹ)
- Tiếng Ả Rập (Algeria, Morocco, Tunis; bố cục AZERTY)
- Tiếng Tây Ban Nha (Mỹ Latinh)

- Tiếng Ý
- Tiếng Đức (Đức và Áo)
- Tiếng Đức (Thụy Sĩ)
- Tiếng Bồ Đào Nha (Brazil, bố cục ABNT2)
- Tiếng Nga (cho bàn phím IBM / Windows 105 phím với bố cục QWERTY)
- Tiếng Thổ Nhĩ Kỳ (bố cục QWERTY)
- Tiếng Pháp (Pháp)
- Tiếng Pháp (Thụy Sĩ)
- Tiếng Pháp (Bỉ, bố cục AZERTY)
- Tiếng Nhật (cho bàn phím 106 phím với bố cục QWERTY)

Một bố cục bàn phím sẽ có thể được sử dụng trong Authentication Agent nếu bố cục này đã được thêm vào cấu hình tiêu chuẩn ngôn ngữ và khu vực của hệ điều hành và có thể được sử dụng trên màn hình chào đón của Microsoft Windows.

Nếu tên tài khoản Authentication Agent chứa các ký hiệu không thể được nhập sử dụng bố cục bàn phím có trong Authentication Agent, ổ cứng được mã hóa sẽ chỉ có thể được truy cập sau khi chúng đã được khôi phục sử dụng Tiện ích Khôi phục hoặc sau khi tên tài khoản Authentication Agent và mật khẩu đã được khôi phục.

Kaspersky Endpoint Security hỗ trợ các loại token, đầu đọc thẻ thông minh và thẻ thông minh sau:

- SafeNet eToken PRO 64K (4.2b) (USB)
- SafeNet eToken PRO 72K Java (USB)
- SafeNet eToken PRO 72K Java (Thẻ thông minh)
- SafeNet eToken 4100 72K Java (Thẻ thông minh)
- SafeNet eToken 5100 (USB)
- SafeNet eToken 5105 (USB)
- SafeNet eToken 7300 (USB)
- EMC RSA SecurID 800 (USB).
- Rutoken EDS (USB)
- Rutoken EDS (Flash)
- Aladdin-RD JaCarta PKI (USB)

- Aladdin-RD JaCarta PKI (Thẻ thông minh)
- Athena IDProtect Laser (USB)
- Gemalto IDBridge CT40 (Đầu đọc thẻ)
- Gemalto IDPrime .NET 511

Mã hóa các ổ cứng sử dụng công nghệ Kaspersky Disk Encryption

Trước khi mã hóa các ổ cứng trên một máy tính, bạn nên đảm bảo rằng máy tính đang không bị nhiễm virus. Để làm điều này, bắt đầu tác vụ Quét Toàn bộ hoặc Quét Khu vực Thiết yếu. Việc mã hóa ổ cứng của một máy tính bị nhiễm rootkit có thể dẫn đến máy ngừng hoạt động.

Để mã hóa các ổ cứng sử dụng công nghệ Kaspersky Disk Encryption:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, mở thư mục với tên của nhóm quản trị mà bạn muốn thiết lập việc mã hóa các ổ cứng.
3. Trong không gian làm việc, chọn thẻ **Chính sách**.
4. Chọn chính sách cần thiết.
5. Mở cửa sổ **Thuộc tính: <Tên chính sách>** sử dụng một trong những phương pháp sau đây:
   - Trong menu ngữ cảnh của chính sách, chọn **Thuộc tính**.
   - Nhấn vào liên kết **Thiết lập chính sách** được đặt ở phần bên phải của không gian làm việc của Bảng điều khiển Quản trị.
6. Trong mục **Mã hóa dữ liệu**, chọn mục con **Mã hóa ổ đĩa cứng**.
7. Trong danh sách thả xuống **Công nghệ mã hóa**, chọn mục **Kaspersky Disk Encryption**.

   Công nghệ Kaspersky Disk Encryption không thể được sử dụng nếu máy tính có các ổ cứng được mã hóa bởi BitLocker.

8. Trong danh sách thả xuống **Chế độ mã hóa**, chọn mục **Mã hóa ổ đĩa cứng**.

   Nếu bạn muốn loại trừ một số ổ cứng khỏi tác vụ mã hóa, hãy tạo một danh sách các ổ cứng đó.

9. Chọn một trong các phương thức mã hóa sau:
   - Nếu bạn muốn chỉ áp dụng mã hóa cho các khu vực ổ cứng có chứa tập tin, chọn hộp kiểm **Chỉ mã hóa dung lượng ổ đĩa được sử dụng**.

Nếu bạn đang áp dụng mã hóa trên một ổ đĩa đang được sử dụng, bạn nên mã hóa toàn bộ ổ đĩa. Điều này đảm bảo mọi dữ liệu đều được bảo vệ - kể cả những dữ liệu đã bị xóa có thể vẫn chứa thông tin truy hồi được. Chức năng **Chỉ mã hóa dung lượng ổ đĩa được sử dụng** được khuyến nghị cho các ổ đĩa mới chưa được sử dụng trước đây.

- Nếu bạn muốn áp dụng mã hóa cho toàn bộ ổ cứng, xóa hộp kiểm **Chỉ mã hóa dung lượng ổ đĩa được sử dụng**.

  Chức năng này chỉ được áp dụng cho các thiết bị chưa được mã hóa. Nếu một thiết bị đã được mã hóa từ trước sử dụng chức năng **Chỉ mã hóa dung lượng ổ đĩa được sử dụng**, sau khi áp dụng một chính sách trong chế độ **Mã hóa tất cả ổ đĩa cứng**, các khu vực không chứa tập tin vẫn sẽ không được mã hóa.

10. Nhấn **OK** để lưu thay đổi.

11. Áp dụng chính sách.

    Xem *Hướng dẫn dành cho Quản trị viên Kaspersky Security Center* để biết chi tiết về việc áp dụng các chính sách Kaspersky Security Center.

Mã hóa ổ cứng sử dụng công nghệ Mã hóa Ổ đĩa BitLocker

Trước khi mã hóa các ổ cứng trên một máy tính, bạn nên đảm bảo rằng máy tính đang không bị nhiễm virus. Để làm điều này, bắt đầu tác vụ Quét Toàn bộ hoặc Quét Khu vực Thiết yếu. Việc mã hóa ổ cứng của một máy tính bị nhiễm rootkit có thể dẫn đến máy ngừng hoạt động.

Việc sử dụng công nghệ BitLocker Drive Encryption trên các máy tính với một hệ điều hành máy chủ có thể yêu cầu cài đặt thành phần **BitLocker Drive Encryption** sử dụng trình hướng dẫn Bổ sung vai trò và thành phần.

Để mã hóa ổ cứng sử dụng công nghệ Mã hóa Ổ đĩa BitLocker:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.

2. Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, mở thư mục với tên của nhóm quản trị mà bạn muốn thiết lập việc mã hóa các ổ cứng.

3. Trong không gian làm việc, chọn thẻ **Chính sách**.

4. Chọn chính sách cần thiết.

5. Mở cửa sổ **Thuộc tính: <Tên chính sách>** sử dụng một trong những phương pháp sau đây:

   - Trong menu ngữ cảnh của chính sách, chọn **Thuộc tính**.

   - Nhấn vào liên kết **Thiết lập chính sách** được đặt ở phần bên phải của không gian làm việc của Bảng điều khiển Quản trị.

6. Trong mục **Mã hóa dữ liệu**, chọn mục con **Mã hóa ổ đĩa cứng**.

7. Trong danh sách thả xuống **Công nghệ mã hóa**, chọn mục **BitLocker Drive Encryption**.

8. Trong danh sách thả xuống **Chế độ mã hóa**, chọn mục **Mã hóa tất cả ổ đĩa cứng**.

9. Nếu bạn muốn sử dụng một bàn phím cảm ứng để nhập thông tin trong một môi trường tiền khởi động, chọn hộp kiểm **Cho phép sử dụng các biện pháp xác thực đòi hỏi nhập liệu từ bàn phím tiền khởi động trên máy tính bảng**.

   Bạn được khuyến nghị chỉ sử dụng cấu hình này cho các thiết bị sử dụng công cụ nhập liệu thay thế ví dụ như một bàn phím USB trong môi trường tiền khởi động.

10. Chọn một trong các kiểu mã hóa sau:

    - Nếu bạn muốn sử dụng mã hóa phần cứng, chọn hộp kiểm **Sử dụng mã hóa phần cứng**.
    - Nếu bạn muốn sử dụng mã hóa phần mềm, xóa hộp kiểm **Sử dụng mã hóa phần cứng**.

11. Chọn một trong các phương thức mã hóa sau:

    - Nếu bạn muốn chỉ áp dụng mã hóa cho các khu vực ổ cứng có chứa tập tin, chọn hộp kiểm **Chỉ mã hóa dung lượng ổ đĩa được sử dụng**.
    - Nếu bạn muốn áp dụng mã hóa cho toàn bộ ổ cứng, xóa hộp kiểm **Chỉ mã hóa dung lượng ổ đĩa được sử dụng**.

      Chức năng này chỉ được áp dụng cho các thiết bị chưa được mã hóa. Nếu một thiết bị đã được mã hóa từ trước sử dụng chức năng **Chỉ mã hóa dung lượng ổ đĩa được sử dụng**, sau khi áp dụng một chính sách trong chế độ **Mã hóa tất cả ổ đĩa cứng**, các khu vực không chứa tập tin vẫn sẽ không được mã hóa.

12. Chọn một phương thức để truy cập ổ cứng được mã hóa với BitLocker.

    - Nếu bạn muốn sử dụng một Mô-đun Nền tảng Đáng Tin cậy (TPM) để lưu trữ các khóa mã hóa, chọn mục **Sử dụng Trusted Platform Module (TPM)**.
    - Nếu bạn không sử dụng một Mô-đun Nền tảng Đáng Tin cậy (TPM) để mã hóa ổ cứng, chọn mục **Sử dụng mật khẩu**, và quy định độ dài ký tự tối thiểu mà một mật khẩu cần chứa trong trường **Độ dài tối thiểu của mật khẩu**.

    Sự khả dụng của một Mô-đun Nền tảng Đáng Tin cậy (TPM) là bắt buộc cho các hệ điều hành Windows 7 và Windows 2008 R2, cũng như cho các phiên bản cũ hơn.

13. Nếu bạn đã chọn mục **Sử dụng Trusted Platform Module (TPM)** ở bước trước:

    - Nếu bạn muốn thiết lập một mã PIN sẽ được yêu cầu khi người dùng cố gắng truy cập một khóa mã hóa, chọn hộp kiểm **Sử dụng PIN** và trong trường **Độ dài PIN tối thiểu**, quy định số chữ số tối thiểu mà một mã PIN cần phải chứa.
    - Nếu bạn muốn truy cập đến các ổ cứng được mã hóa trên máy tính không có một mô-đun nền tảng đáng tin cậy sử dụng mật khẩu, chọn hộp kiểm **Sử dụng mật khẩu nếu Trusted Platform Module (TPM) không khả dụng**, và trong trường **Độ dài tối thiểu của mật khẩu**, quy định số ký tự tối thiểu mà một mật khẩu nên chứa.

Trong trường hợp này, việc truy cập đến các khóa mã hóa sẽ xảy ra sử dụng mật khẩu được quy định, như khi hộp kiểm **Sử dụng mật khẩu** được chọn.

Nếu hộp kiểm **Sử dụng mật khẩu nếu Trusted Platform Module (TPM) không khả dụng** không được chọn và một mô-đun nền tảng đáng tin cậy không khả dụng, tác vụ mã hóa ổ cứng sẽ không được bắt đầu.

14. Nhấn **OK** để lưu thay đổi.

15. Áp dụng chính sách.

    Xem *Hướng dẫn dành cho Quản trị viên Kaspersky Security Center* để biết chi tiết về việc áp dụng các chính sách Kaspersky Security Center.

Sau khi áp dụng chính sách trên máy khách có cài đặt Kaspersky Endpoint Security, các truy vấn sau sẽ được thực hiện:

- Nếu chính sách mã hóa được áp dụng cho một ổ cứng hệ thống, cửa sổ mã PIN sẽ xuất hiện nếu mô-đun nền tảng đáng tin cậy đang được sử dụng, hoặc nếu không, cửa sổ yêu cầu mật khẩu sẽ xuất hiện để tải trước xác thực.

- Nếu hệ điều hành của máy tính được bật chế độ tương thích tiêu chuẩn Xử lý Thông tin Liên bang, thì trong Windows 8 và các hệ điều hành cao hơn, một cửa sổ yêu cầu kết nối thiết bị USB sẽ được hiển thị để lưu tập tin khóa phục hồi.

Nếu không có truy cập đến các khóa mã hóa, người dùng có thể yêu cầu quản trị viên mạng cục bộ cung cấp một khóa phục hồi (nếu khóa phục hồi đã không được lưu trước đó trên thiết bị USB, hoặc đã bị thất lạc).

Tạo một danh sách các ổ cứng được loại trừ khỏi tác vụ mã hóa

Bạn có thể tạo một danh sách loại trừ khỏi tác vụ mã hóa chỉ dành cho công nghệ Kaspersky Disk Encryption.

Để tạo một danh sách các ổ cứng được loại trừ khỏi tác vụ mã hóa:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.

2. Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, mở thư mục với tên của nhóm quản trị mà bạn muốn tạo một danh sách ổ cứng được loại trừ khỏi tác vụ mã hóa.

3. Trong không gian làm việc, chọn thẻ **Chính sách**.

4. Chọn chính sách cần thiết.

5. Mở cửa sổ **Thuộc tính: <Tên chính sách>** sử dụng một trong những phương pháp sau đây:

   - Trong menu ngữ cảnh của chính sách, chọn **Thuộc tính**.

   - Nhấn vào liên kết **Thiết lập chính sách** được đặt ở phần bên phải của không gian làm việc của Bảng điều khiển Quản trị.

6. Trong mục **Mã hóa dữ liệu**, chọn mục con **Mã hóa ổ đĩa cứng**.

7. Trong danh sách thả xuống **Công nghệ mã hóa**, chọn mục **Kaspersky Disk Encryption**.

   Các mục tương ứng với ổ cứng được loại trừ khỏi tác vụ mã hóa sẽ xuất hiện trong bảng **Không mã hóa ổ đĩa cứng sau đây**. Bảng này sẽ trống nếu trước đó bạn chưa tạo một danh sách ổ cứng được loại trừ khỏi tác vụ mã hóa.

8. Để thêm ổ cứng vào danh sách các ổ cứng được loại trừ khỏi tác vụ mã hóa:

   a. Nhấn vào nút **Thêm**.

      Cửa sổ **Thêm các thiết bị vào danh sách Kaspersky Security Center** sẽ được mở ra.

   b. Trong cửa sổ **Thêm các thiết bị vào danh sách Kaspersky Security Center**, quy định giá trị của các tham số sau: **Tên**, **Máy tính**, **Kiểu ổ đĩa**, và **Kaspersky Disk Encryption**.

   c. Nhấn vào nút **Làm mới**.

   d. Trong cột **Tên**, chọn hộp kiểm trong các hàng tương ứng với các ổ cứng mà bạn muốn bổ sung vào danh sách các ổ cứng được loại trừ khỏi tác vụ mã hóa.

   e. Nhấn **OK**.

   Các ổ cứng được chọn sẽ xuất hiện trong bảng **Không mã hóa các ổ cứng sau**.

9. Nếu bạn muốn xóa các ổ cứng khỏi bảng loại trừ, chọn một hoặc nhiều dòng trong bảng **Không mã hóa ổ đĩa cứng sau đây** và nhấn nút **Gỡ bỏ**.

   Để chọn nhiều dòng trong bảng, giữ nút **CTRL** khi chọn chúng.

10. Nhấn **OK** để lưu thay đổi.

Giải mã ổ cứng

Bạn có thể giải mã các ổ cứng đã được mã hóa kể cả khi không có một giấy phép còn hiệu lực cho phép việc mã hóa dữ liệu.

Để giải mã các ổ cứng:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.

2. Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, mở thư mục với tên của nhóm quản trị mà bạn muốn thiết lập việc giải mã các ổ cứng.

3. Trong không gian làm việc, chọn thẻ **Chính sách**.

4. Chọn chính sách cần thiết.

5. Mở cửa sổ **Thuộc tính: <Tên chính sách>** sử dụng một trong những phương pháp sau đây:

   - Trong menu ngữ cảnh của chính sách, chọn **Thuộc tính**.

- Nhấn vào liên kết **Thiết lập chính sách** được đặt ở phần bên phải của không gian làm việc của Bảng điều khiển Quản trị.

6. Trong mục **Mã hóa dữ liệu**, chọn mục con **Mã hóa ổ đĩa cứng**.
7. Trong danh sách thả xuống **Công nghệ mã hóa**, chọn công nghệ đã được sử dụng để mã hóa ổ cứng.
8. Thực hiện một trong các thao tác sau:
   - Trong danh sách thả xuống **Chế độ mã hóa**, chọn mục **Lựa chọn tất cả đĩa cứng** nếu bạn muốn giải mã tất cả các ổ cứng được mã hóa.
   - Thêm ổ cứng được mã hóa mà bạn muốn giải mã vào bảng **Không mã hóa ổ đĩa cứng sau đây**.

     Tùy chọn này chỉ có thể được sử dụng cho công nghệ Kaspersky Disk Encryption.
9. Nhấn **OK** để lưu thay đổi.
10. Áp dụng chính sách.

    Xem *Hướng dẫn dành cho Quản trị viên Kaspersky Security Center* để biết chi tiết về việc áp dụng các chính sách Kaspersky Security Center.

Nếu người dùng tắt hoặc khởi động lại máy tính trong quá trình giải mã ổ cứng đã được mã hóa sử dụng công nghệ Kaspersky Disk Encryption, Authentication Agent sẽ được nạp trước lần khởi động hệ điều hành tiếp theo. Kaspersky Endpoint Security sẽ tiếp tục quá trình giải mã ổ cứng sau khi xác thực thành công trong authentication agent và trong quá trình khởi động hệ điều hành.

Nếu hệ điều hành được chuyển sang chế độ ngủ đông trong quá trình giải mã các ổ cứng đã được mã hóa sử dụng công nghệ Kaspersky Disk Encryption, Authentication Agent sẽ được nạp khi hệ điều hành ra khỏi chế độ ngủ đông. Kaspersky Endpoint Security sẽ tiếp tục quá trình giải mã ổ cứng sau khi xác thực thành công trong authentication agent và trong quá trình khởi động hệ điều hành. Sau khi giải mã ổ cứng, chế độ ngủ đông sẽ không thể được sử dụng cho đến lần khởi động lại đầu tiên của hệ điều hành.

Nếu hệ điều hành chuyển sang chế độ ngủ trong quá trình giải mã ổ cứng, Kaspersky Endpoint Security sẽ tiếp tục giải mã ổ cứng khi hệ điều hành ra khỏi chế độ ngủ mà không nạp Authentication Agent.

Quản lý Authentication Agent

Nếu ổ cứng hệ thống được mã hóa, Authentication Agent sẽ được nạp trước khi khởi động hệ điều hành. Sử dụng Authentication Agent để hoàn tất quá trình xác thực và nhận quyền truy cập đến các ổ cứng hệ thống được mã hóa và nạp hệ điều hành.

Sau khi hoàn tất thủ tục xác thực, hệ điều hành sẽ được nạp. Tiến trình xác thực sẽ được lặp lại mỗi lần hệ điều hành khởi động lại.

Người dùng có thể sẽ không thể hoàn tất quá trình xác thực trong một số trường hợp. Ví dụ, việc xác thực không thể được thực hiện nếu người dùng đã quên thông tin tài khoản của tài khoản Authentication Agent, hoặc mật khẩu cho token hoặc thẻ thông minh, hoặc đã làm mất token hoặc thẻ thông minh.

Nếu người dùng đã quên thông tin của tài khoản Authentication Agent, hoặc mật khẩu cho token hoặc thẻ thông minh, bạn phải liên hệ với quản trị viên mạng LAN doanh nghiệp để phục hồi chúng.

Nếu người dùng đã làm mất token hoặc thẻ thông minh, quản trị viên sẽ phải bổ sung tập tin của một chứng chỉ điện tử token hoặc thẻ thông minh vào lệnh tạo một tài khoản Authentication Agent. Sau đó, người dùng phải hoàn tất thủ tục khôi phục dữ liệu trên các thiết bị được mã hóa.

Sử dụng token và thẻ thông minh với Authentication Agent

Một token hoặc thẻ thông minh có thể được sử dụng để xác thực khi truy cập các ổ cứng được mã hóa. Để làm điều này, bạn phải bổ sung tập tin của một chứng chỉ điện tử token hoặc thẻ thông minh vào lệnh tạo một tài khoản Authentication Agent.

Việc sử dụng token hoặc thẻ thông minh chỉ có thể được thực hiện nếu ổ cứng của máy tính đã được mã hóa sử dụng thuật toán mã hóa AES256. Nếu ổ cứng của máy tính đã được mã hóa sử dụng thuật toán mã hóa AES56, việc bổ sung tập tin chứng chỉ điện tử đến lệnh sẽ bị từ chối.

Để bổ sung tập tin của một chứng chỉ điện tử token hoặc thẻ thông minh vào lệnh tạo một tài khoản Authentication Agent, trước hết bạn phải lưu tập tin đó sử dụng một phần mềm thuộc bên thứ ba chuyên quản lý chứng chỉ.

Chứng chỉ token hoặc thẻ thông minh phải có các thuộc tính sau:

- Chứng chỉ phải tuân thủ tiêu chuẩn X.509, và tập tin chứng chỉ phải có mã hóa văn bản DER.

  Nếu chứng chỉ điện tử của token hoặc thẻ thông minh không đáp ứng được yêu cầu này, tiện ích quản trị sẽ không nạp tập tin của chứng chỉ này vào lệnh tạo tài khoản Authentication Agent và hiển thị một thông báo lỗi.

- Tham số `KeyUsage` quy định mục đích của chứng chỉ phải có giá trị `keyEncipherment` hoặc `dataEncipherment`.

  Nếu chứng chỉ điện tử của token hoặc thẻ thông minh không đáp ứng được yêu cầu này, tiện ích quản trị sẽ nạp tập tin của chứng chỉ này vào lệnh tạo tài khoản Authentication Agent và hiển thị một cảnh báo.

- Chứng chỉ chứa một khóa RSA với độ dài ít nhất 1024 bit.

  Nếu chứng chỉ điện tử của token hoặc thẻ thông minh không đáp ứng được yêu cầu này, tiện ích quản trị sẽ không nạp tập tin của chứng chỉ này vào lệnh tạo tài khoản Authentication Agent và hiển thị một thông báo lỗi.

Sửa thông điệp trợ giúp của Authentication Agent

Trước khi sửa các thông điệp trợ giúp của Authentication Agent, hãy xem lại danh sách các ký tự được hỗ trợ trong môi trường tiền khởi động.

Để sửa thông điệp trợ giúp của Authentication Agent:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, mở thư mục với tên của nhóm quản trị mà bạn muốn sửa thông điệp trợ giúp của Authentication Agent.
3. Trong không gian làm việc, chọn thẻ **Chính sách**.

4. Chọn chính sách cần thiết.
5. Mở cửa sổ **Thuộc tính: <Tên chính sách>** sử dụng một trong những phương pháp sau đây:
   - Trong menu ngữ cảnh của chính sách, chọn **Thuộc tính**.
   - Nhấn vào liên kết **Thiết lập chính sách** được đặt ở phần bên phải của không gian làm việc của Bảng điều khiển Quản trị.
6. Trong mục **Mã hóa dữ liệu**, chọn mục con **Cấu hình mã hóa chung**.
7. Trong mục **Mẫu**, chọn nút **Trợ giúp**.
   Việc này sẽ mở ra cửa sổ **Tin nhắn trợ giúp Authentication Agent**.
8. Làm các bước sau:
   - Chọn thẻ **Chứng thực** để sửa văn bản trợ giúp được hiển thị trong cửa sổ Authentication Agent khi dữ liệu xác thực tài khoản đang được nhập.
   - Chọn thẻ **Thay đổi mật khẩu** để sửa văn bản trợ giúp được hiển thị trong cửa sổ Authentication Agent khi mật khẩu cho tài khoản Authentication Agent đang được thay đổi.
   - Chọn thẻ **Khôi phục mật khẩu** để sửa văn bản trợ giúp được hiển thị trong cửa sổ Authentication Agent khi mật khẩu cho tài khoản Authentication Agent đang được khôi phục.
9. Sửa thông điệp trợ giúp.
   Nếu bạn muốn khôi phục văn bản gốc, nhấn nút **Mặc định**.
10. Nhấn **OK**.
11. Để lưu thay đổi của bạn, trong cửa sổ **Thuộc tính: <Tên chính sách>**, nhấn **OK**.

Hỗ trợ hạn chế cho các ký tự trong thông điệp trợ giúp của Authentication Agent

Trong một môi trường tiền khởi động, các ký tự Unicode sau được hỗ trợ:

- Ký tự alphabet Latinh cơ bản (0000 - 007F)
- Ký tự Latin-1 Bổ sung (0080 - 00FF)
- Latin-A Mở rộng (0100 - 017F)
- Latin-B Mở rộng (0180 - 024F)
- Các ký tự ID mở rộng không kết hợp (02B0 - 02FF)
- Các bộ dấu kết hợp (0300 - 036F)
- Bảng alphabet Hy Lạp và Coptic (0370 - 03FF)
- Cyrillic (0400 - 04FF)

- Do Thái (0590 - 05FF)
- Chữ Ả Rập (0600 - 06FF)
- Latinh mở rộng bổ sung (1E00 - 1EFF)
- Dấu câu (2000 - 206F)
- Biểu tượng tiền tệ (20A0 - 20CF)
- Biểu tượng giống chữ cái (2100 - 214F)
- Hình học (25A0 - 25FF)
- Dạng trình bày của Kịch bản Ả Rập B (FE70 - FEFF)

Các ký tự không được quy định trong danh sách này đều không được hỗ trợ trong môi trường tiền khởi động. Bạn không nên sử dụng các ký tự đó trong thông điệp trợ giúp của Authentication Agent.

Chọn cấp độ ghi nhận dấu vết Authentication Agent

Ứng dụng ghi lại thông tin dịch vụ về hoạt động của Authentication Agent và thông tin về hoạt động của người dùng với Authentication Agent trong tập tin dấu vết. Tập tin dấu vết Authentication Agent sẽ rất hữu ích khi bạn cần khôi phục dữ liệu trên các ổ cứng được mã hóa.

Để chọn cấp độ ghi nhận dấu vết Authentication Agent:

1. Ngay khi máy tính với một ổ cứng được mã hóa được khởi động, hãy nhấn phím **F3** để gọi một cửa sổ thiết lập cấu hình Authentication Agent.
2. Chọn cấp độ ghi nhận dấu vết trong cửa sổ cấu hình Authentication Agent:
   - **Tắt nhật ký gỡ lỗi (mặc định)**. Nếu chọn tùy chọn này, ứng dụng sẽ không ghi lại thông tin về các sự kiện Authentication Agent trong tập tin dấu vết.
   - **Bật nhật ký gỡ lỗi**. Nếu tùy chọn này được chọn, ứng dụng sẽ ghi lại thông tin về hoạt động của Authentication Agent và các hoạt động của người dùng với Authentication Agent trong tập tin dấu vết.
   - **Bật nhật ký đầy đủ**. Nếu tùy chọn này được chọn, ứng dụng sẽ ghi lại thông tin chi tiết về hoạt động của Authentication Agent và các hoạt động của người dùng với Authentication Agent trong tập tin dấu vết.

     Cấp độ chi tiết của các đề mục trong tùy chọn này là cao hơn so với cấp độ của tùy chọn **Bật nhật ký gỡ lỗi**. Một cấp độ chi tiết cao có thể làm chậm việc khởi động của Authentication Agent và hệ điều hành.

   - **Bật nhật ký gỡ lỗi và chọn cổng serial**. Nếu tùy chọn này được chọn, ứng dụng sẽ ghi lại thông tin về hoạt động của Authentication Agent và các hoạt động của người dùng với Authentication Agent trong tập tin dấu vết, và chuyển tiếp nó qua cổng COM.

Nếu một máy tính với ổ cứng được mã hóa được kết nối đến một máy tính khác qua cổng COM, các sự kiện Authentication Agent có thể được kiểm tra từ máy tính khác đó.

- **Bật nhật ký gỡ lỗi đầy đủ và chọn cổng serial**. Nếu tùy chọn này được chọn, ứng dụng sẽ ghi lại thông tin chi tiết về hoạt động của Authentication Agent và các hoạt động của người dùng với Authentication Agent trong tập tin dấu vết, và chuyển tiếp nó qua cổng COM.

  Cấp độ chi tiết của các đề mục trong tùy chọn này là cao hơn so với cấp độ của tùy chọn **Bật nhật ký gỡ lỗi và chọn cổng serial**. Một cấp độ chi tiết cao có thể làm chậm việc khởi động của Authentication Agent và hệ điều hành.

Dữ liệu sẽ được ghi trong tập tin dấu vết Authentication Agent nếu có các ổ cứng được mã hóa trên máy tính hoặc trong quá trình mã hóa ổ cứng.

Tập tin dấu vết Authentication Agent sẽ không được gửi đến Kaspersky, trái với các tập tin dấu vết khác của ứng dụng. Nếu cần, quản trị viên hệ thống có thể gửi thủ công tập tin dấu vết Authentication Agent đến Kaspersky để phân tích.

Quản lý tài khoản Authentication Agent

Các công cụ Kaspersky Security Center sau đây có thể được sử dụng để quản lý tài khoản Authentication Agent:

- Tác vụ nhóm để quản lý tài khoản Authentication Agent. Tác vụ này cho phép bạn quản lý các tài khoản Authentication Agent cho một nhóm các máy khách.
- Tác vụ cục bộ **Mã hóa (quản lý tài khoản)**. Tác vụ này cho phép bạn quản lý các tài khoản Authentication Agent cho các máy khách riêng lẻ.

Để thiết lập cấu hình cho tác vụ quản lý tài khoản Authentication Agent:

1. Tạo (Tạo một tác vụ cục bộ, Tạo một tác vụ nhóm) một tác vụ quản lý tài khoản Authentication Agent.
2. Mở mục **Cấu hình** trong cửa sổ **Thuộc tính: <tên của tác vụ quản lý tài khoản Authentication Agent>**.
3. Bổ sung các lệnh để tạo tài khoản Authentication Agent.
4. Bổ sung các lệnh để sửa tài khoản Authentication Agent.
5. Bổ sung các lệnh để xóa tài khoản người dùng Authentication Agent.
6. Nếu cần thiết, sửa lệnh được bổ sung để quản lý các tài khoản Authentication Agent. Để làm điều này, chọn một lệnh trong bảng **Lệnh để quản lý tài khoản Authentication Agent** và nhấn nút **Chỉnh sửa**.
7. Nếu cần thiết, xóa lệnh được bổ sung để quản lý các tài khoản Authentication Agent. Để làm điều này, chọn một hoặc nhiều lệnh trong bảng **Lệnh để quản lý các tài khoản Authentication Agent** và nhấn nút **Gỡ bỏ**.

   Để chọn nhiều dòng trong bảng, giữ nút **CTRL** khi chọn chúng.

8. Để lưu lại thay đổi, chọn **OK** trong cửa sổ thuộc tính của tác vụ.

9. Chạy tác vụ.

Các lệnh quản lý tài khoản Authentication Agent được bổ sung vào tác vụ sẽ được thực thi.

Bổ sung một lệnh để tạo một tài khoản Authentication Agent

Để bổ sung một lệnh để tạo một tài khoản Authentication Agent:

1. Mở mục **Cấu hình** trong cửa sổ **Thuộc tính: <tên của tác vụ quản lý tài khoản Authentication Agent>**.

2. Nhấn nút **Thêm**, và trong danh sách thả xuống chọn **Lệnh thêm tài khoản**.

   Cửa sổ **Thêm tài khoản người dùng** sẽ được mở ra.

3. Trong trường **Thêm tài khoản người dùng** của cửa sổ **Tài khoản Windows**, quy định tên tài khoản Microsoft Windows mà dựa vào đó tài khoản Authentication Agent sẽ được tạo.

   Để làm việc này, nhập tên tài khoản một cách thủ công hoặc nhấn nút **Lựa chọn**.

4. Nếu bạn đã nhập thủ công tên của một tài khoản Microsoft Windows, nhấn nút **Cho phép** để xác định định danh bảo mật (SID) của tài khoản.

   Nếu bạn không muốn xác định định danh bảo mật (SID) bằng cách nhấn nút **Cho phép**, nó sẽ được xác định khi tác vụ được thực hiện trên máy tính.

   > Việc xác định SID của một tài khoản Microsoft Windows khi bổ sung lệnh tạo tài khoản Authentication Agent là một cách rất tiện lợi để đảm bảo tên tài khoản Microsoft Windows đã được nhập thủ công chính xác. Nếu tài khoản người dùng Microsoft Windows được nhập không tồn tại, thuộc một miền không tin tưởng, hoặc không có trên máy tính mà tác vụ cục bộ **Mã hóa (quản lý tài khoản)** đang được thay đổi, tác vụ quản lý tài khoản Authentication Agent sẽ kết thúc với lỗi.

5. Chọn hộp kiểm 更改当前用户账户 để thay thế một tài khoản có tên tương tự đã được tạo từ trước cho Authentication Agent với tài khoản đang được tạo.

   > Bước này có thể được sử dụng khi bạn bổ sung một lệnh tạo tài khoản Authentication Agent trong thuộc tính của một tác vụ nhóm cho việc quản lý các tài khoản Authentication Agent. Bước này không thể được sử dụng nếu bạn đang bổ sung một lệnh tạo tài khoản Authentication Agent trong thuộc tính của một tác vụ cục bộ **Mã hóa (quản lý tài khoản)**.

6. Trong trường **Tên người dùng**, nhập tên của tài khoản Authentication Agent phải được nhập trong quá trình xác thực để truy cập vào các ổ cứng được mã hóa.

7. Chọn hộp kiểm **Cho phép xác thực dựa trên mật khẩu** nếu bạn muốn ứng dụng nhắc người dùng nhập mật khẩu của tài khoản Authentication Agent trong quá trình xác thực để truy cập các ổ cứng được mã hóa.

8. Nếu bạn đã chọn hộp kiểm **Cho phép xác thực dựa trên mật khẩu** ở bước trước:

   a. Trong trường **Mật khẩu**, nhập mật khẩu của tài khoản Authentication Agent phải được nhập trong quá trình xác thực để truy cập vào các ổ cứng được mã hóa.

b. Trong trường **Xác nhận mật khẩu**, xác nhận mật khẩu của tài khoản Authentication Agent được nhập ở bước trước.

c. Thực hiện một trong các thao tác sau:

- Chọn mục **Thay đổi mật khẩu khi chứng thực lần đầu tiên** nếu bạn muốn ứng dụng hiển thị một yêu cầu thay đổi mật khẩu cho người dùng vượt qua quá trình xác thực theo tài khoản được quy định ở dòng lệnh ở lần đầu tiên.
- Nếu không, chọn mục **Không yêu cầu thay đổi mật khẩu**.

9. Chọn hộp kiểm **Cho phép xác thực dựa trên chứng nhận** nếu bạn muốn ứng dụng nhắc người dùng kết nối một token hoặc thẻ thông minh đến máy tính trong quá trình xác thực để truy cập các ổ cứng được mã hóa.

10. Nếu bạn đã chọn hộp kiểm **Cho phép xác thực dựa trên chứng nhận** ở bước trước, nhấn nút **Duyệt** và chọn tập tin của chứng chỉ điện tử token hoặc thẻ thông minh trong cửa sổ **Lựa chọn tập tin chứng nhận**.

11. Nếu cần thiết, trong trường **Mô tả dòng lệnh**, nhập chi tiết tài khoản Authentication Agent mà bạn cần để quản lý lệnh.

12. Thực hiện một trong các thao tác sau:

- Chọn hộp kiểm **Cho phép chứng thực** nếu bạn muốn ứng dụng cho phép người dùng sử dụng tài khoản được quy định trong dòng lệnh được truy cập hộp thoại xác thực trong Authentication Agent.
- Chọn hộp kiểm **Ngăn chặn chứng thực** nếu bạn muốn ứng dụng chặn người dùng sử dụng tài khoản được quy định trong dòng lệnh khỏi truy cập hộp thoại xác thực trong Authentication Agent.

13. Trong cửa sổ **Thêm tài khoản người dùng**, nhấn **OK**.

Bổ sung một lệnh sửa tài khoản Authentication Agent

Để bổ sung một lệnh để sửa một tài khoản Authentication Agent:

1. Trong mục **Cấu hình** của cửa sổ **Thuộc tính: <tên của tác vụ quản lý tài khoản Authentication Agent>**, mở menu ngữ cảnh của nút **Thêm** và chọn mục **Lệnh chỉnh sửa tài khoản**.

   Cửa sổ **Chỉnh sửa tài khoản người dùng** sẽ được mở ra.

2. Trong trường **Tài khoản Windows** của cửa sổ **Chỉnh sửa tài khoản người dùng**, quy định tên tài khoản Microsoft Windows đã được sử dụng để tạo tài khoản Authentication Agent mà bạn muốn sửa. Để làm việc này, nhập tên tài khoản một cách thủ công hoặc nhấn nút **Lựa chọn**.

3. Nếu bạn đã nhập thủ công tên của một tài khoản Microsoft Windows, nhấn nút **Cho phép** để xác định định danh bảo mật (SID) của tài khoản.

   Nếu bạn không muốn xác định định danh bảo mật (SID) bằng cách nhấn nút **Cho phép**, nó sẽ được xác định khi tác vụ được thực hiện trên máy tính.

Việc xác định SID của một tài khoản Microsoft Windows khi bổ sung lệnh sửa tài khoản Authentication Agent là một cách rất tiện lợi để đảm bảo tên tài khoản Microsoft Windows đã được nhập thủ công chính xác. Nếu tài khoản người dùng Microsoft Windows được nhập không tồn tại hoặc thuộc một miền không tin tưởng, tác vụ nhóm để quản lý các tài khoản Authentication Agent sẽ kết thúc với lỗi.

4. Chọn hộp kiểm **Thay đổi tên người dùng** và nhập một tên mới cho tài khoản Authentication Agent nếu bạn muốn Kaspersky Endpoint Security thay đổi tên người dùng cho tất cả các tài khoản Authentication Agent được tạo sử dụng tài khoản Microsoft Windows với tên được ghi trong trường **Tài khoản Windows** thành tên được nhập vào trường bên dưới.

5. Chọn hộp kiểm **Sửa đổi cấu hình xác thực dựa trên mật khẩu** để có thể sửa cấu hình xác thực bằng mật khẩu.

6. Chọn hộp kiểm **Cho phép xác thực dựa trên mật khẩu** nếu bạn muốn ứng dụng nhắc người dùng nhập mật khẩu của tài khoản Authentication Agent trong quá trình xác thực để truy cập các ổ cứng được mã hóa.

7. Nếu bạn đã chọn hộp kiểm **Cho phép xác thực dựa trên mật khẩu** ở bước trước:

   a. Trong trường **Mật khẩu**, nhập mật khẩu mới của tài khoản Authentication Agent.

   b. Trong trường **Xác nhận mật khẩu**, xác nhận mật khẩu đã được nhập ở bước trước.

8. Chọn hộp kiểm **Chỉnh sửa quy tắc thay đổi mật khẩu khi chứng thực trong Authentication Agent** nếu bạn muốn Kaspersky Endpoint Security thay đổi giá trị của cấu hình thay đổi mật khẩu cho tất cả các tài khoản Authentication Agent được tạo sử dụng tài khoản Microsoft Windows với tên được ghi trong trường **Tài khoản Windows** thành giá trị được nhập dưới đây.

9. Quy định giá trị của cấu hình thay đổi mật khẩu khi xác thực trong Authentication Agent.

10. Chọn hộp kiểm **Sửa đổi cấu hình xác thực dựa trên chứng nhận** để có thể sửa cấu hình xác thực dựa trên chứng chỉ điện tử của một token hoặc thẻ thông minh.

11. Chọn hộp kiểm **Cho phép xác thực dựa trên chứng nhận** nếu bạn muốn ứng dụng nhắc người dùng nhập mật khẩu cho token hoặc thẻ thông minh được kết nối đến máy tính trong quá trình xác thực để có thể truy cập các ổ cứng được mã hóa.

12. Nếu bạn đã chọn hộp kiểm **Cho phép xác thực dựa trên chứng nhận** ở bước trước, nhấn nút **Duyệt** và chọn tập tin của chứng chỉ điện tử token hoặc thẻ thông minh trong cửa sổ **Lựa chọn tập tin chứng nhận**.

13. Chọn hộp kiểm **Chỉnh sửa mô tả dòng lệnh** và sửa mô tả lệnh nếu bạn muốn Kaspersky Endpoint Security thay đổi mô tả lệnh cho tất cả các tài khoản Authentication Agent được tạo sử dụng tài khoản Microsoft Windows với tên được ghi trong trường **Tài khoản Windows**.

14. Chọn hộp kiểm **Chỉnh sửa quy tắc chứng thực truy cập trong Authentication Agent** nếu bạn muốn Kaspersky Endpoint Security thay đổi quy tắc truy cập hộp thoại xác thực trong Authentication Agent đến giá trị được quy định dưới đây cho tất cả các tài khoản Authentication Agent được tạo sử dụng tài khoản Microsoft Windows với tên được ghi trong trường **Tài khoản Windows**.

15. Nhập quy tắc để truy cập hộp thoại xác thực trong Authentication Agent.

16. Trong cửa sổ **Chỉnh sửa tài khoản người dùng**, nhấn **OK**.

Bổ sung một lệnh để xóa một tài khoản Authentication Agent

Để bổ sung một lệnh để xóa một tài khoản Authentication Agent:

1. Trong mục **Cấu hình** của cửa sổ **Thuộc tính: <tên của tác vụ quản lý tài khoản Authentication Agent>**, mở menu ngữ cảnh của nút **Thêm** và chọn mục **Lệnh xóa tài khoản**.

   Cửa sổ **Xóa tài khoản người dùng** sẽ được mở ra.

2. Trong trường **Tài khoản Windows** của cửa sổ **Xóa tài khoản người dùng**, quy định tên tài khoản Microsoft Windows đã được sử dụng để tạo tài khoản Authentication Agent mà bạn muốn xóa. Để làm việc này, nhập tên tài khoản một cách thủ công hoặc nhấn nút **Lựa chọn**.

3. Nếu bạn đã nhập thủ công tên của một tài khoản Microsoft Windows, nhấn nút **Cho phép** để xác định định danh bảo mật (SID) của tài khoản.

   Nếu bạn không muốn xác định định danh bảo mật (SID) bằng cách nhấn nút **Cho phép**, nó sẽ được xác định khi tác vụ được thực hiện trên máy tính.

   > Việc xác định SID của một tài khoản Microsoft Windows khi bổ sung lệnh xóa tài khoản Authentication Agent là một cách rất tiện lợi để đảm bảo tên tài khoản Microsoft Windows đã được nhập thủ công chính xác. Nếu tài khoản người dùng Microsoft Windows được nhập không tồn tại hoặc thuộc một miền không tin tưởng, tác vụ nhóm để quản lý các tài khoản Authentication Agent sẽ kết thúc với lỗi.

4. Trong cửa sổ **Xóa tài khoản người dùng**, nhấn **OK**.

Khôi phục chi tiết tài khoản Authentication Agent

> Các chỉ dẫn này dành cho người sử dụng của máy khách có cài đặt Kaspersky Endpoint Security.

Để khôi phục tên người dùng và mật khẩu của một tài khoản Authentication Agent:

1. Authentication Agent sẽ được nạp trên một máy tính có ổ cứng được mã hóa trước khi hệ điều hành được nạp. Trong giao diện của Authentication Agent, nhấn nút **Có phải bạn quên mật khẩu không** để bắt đầu tiến trình khôi phục tên người dùng và mật khẩu của một tài khoản Authentication Agent.

2. Làm theo chỉ dẫn của Authentication Agent để nhận đơn vị yêu cầu khôi phục tên người dùng và mật khẩu của tài khoản Authentication Agent.

3. Đọc nội dung của khối yêu cầu cho quản trị viên mạng LAN của công ty của bạn, cùng với tên của máy tính.

4. Nhập các mục trả lời cho yêu cầu khôi phục tên người dùng và mật khẩu của tài khoản Authentication Agent đã được tạo và cung cấp cho bạn bởi quản trị viên mạng LAN.

5. Nhập một mật khẩu mới cho tài khoản Authentication Agent và xác nhận nó.

   Tên người dùng của tài khoản Authentication Agent được xác định sử dụng các mục trả lời cho yêu cầu khôi phục tên người dùng và mật khẩu của tài khoản Authentication Agent.

Sau khi bạn đã nhập và xác nhận mật khẩu của tài khoản Authentication Agent, mật khẩu sẽ được lưu lại và bạn sẽ được phép truy cập các ổ cứng được mã hóa.

Đáp lại yêu cầu của người dùng để khôi phục chi tiết tài khoản Authentication Agent

Để tạo và gửi đến người dùng các mục trả lời yêu cầu khôi phục tên người dùng và mật khẩu của một tài khoản Authentication Agent:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, mở thư mục với tên của nhóm quản trị chứa máy tính của người dùng đã yêu cầu khôi phục tên người dùng và mật khẩu của một tài khoản Authentication Agent.
3. Trong không gian làm việc, chọn thẻ **Các thiết bị**.
4. Trên thẻ **Các thiết bị**, chọn máy tính của người dùng đã yêu cầu khôi phục tên người dùng và mật khẩu của một tài khoản Authentication Agent và nhấn phải chuột để mở ra menu ngữ cảnh.
5. Trong menu ngữ cảnh, chọn **Cấp quyền truy cập vào thiết bị và các dữ liệu ở chế độ ngoại tuyến**.

   Cửa sổ **Cấp quyền truy cập vào thiết bị và các dữ liệu ở chế độ ngoại tuyến** sẽ được mở ra.
6. Trong cửa sổ **Cấp quyền truy cập vào thiết bị và các dữ liệu ở chế độ ngoại tuyến**, chọn thẻ **Authentication Agent**.
7. Trong cửa sổ **Thuật toán mã hóa được sử dụng**, chọn loại thuật toán mã hóa.
8. Trong danh sách thả xuống **Tài khoản**, chọn tên của tài khoản Authentication Agent được tạo cho người dùng đang yêu cầu khôi phục tên và mật khẩu của tài khoản Authentication Agent.
9. Trong danh sách thả xuống **Ổ đĩa cứng**, chọn ổ cứng được mã hóa mà bạn cần khôi phục truy cập.
10. Trong mục **Người dùng yêu cầu**, nhập khối yêu cầu được đọc bởi người dùng.

    Nội dung của các mục trả lời yêu cầu khôi phục tên người dùng và mật khẩu của một tài khoản Authentication Agent sẽ được hiển thị trong trường **Khóa truy cập**.
11. Đọc nội dung của văn bản trả lời cho người dùng.

Xem chi tiết mã hóa dữ liệu

Mục này mô tả cách bạn có thể xem chi tiết mã hóa dữ liệu.

Thông tin về tình trạng mã hóa

Trong khi tiến trình mã hóa hoặc giải mã đang được thực hiện, Kaspersky Endpoint Security sẽ chuyển tiếp thông tin về tình trạng của các tham số mã hóa được áp dụng cho máy khách đến Kaspersky Security Center.

Các giá trị tình trạng mã hóa sau có thể được sử dụng:

- *Chính sách không được quy định*. Một chính sách Kaspersky Security Center đã không được quy định cho máy tính.
- *Mã hóa / giải mã đang diễn ra*. Tiến trình mã hóa và / hoặc giải mã dữ liệu đang diễn ra trên máy tính.
- *Lỗi*. Có lỗi xảy ra trong quá trình mã hóa và / hoặc giải mã dữ liệu trên máy tính.
- *Yêu cầu khởi động lại*. Hệ điều hành cần được khởi động lại để bắt đầu hoặc hoàn tất quá trình mã hóa hoặc giải mã dữ liệu trên máy tính.
- *Tuân thủ chính sách*. Mã hóa và / hoặc giải mã dữ liệu trên máy tính đã được hoàn tất sử dụng cấu hình mã hóa được quy định trong chính sách Kaspersky Security Center được áp dụng cho máy tính.
- *Hủy bỏ bởi người dùng*. Người dùng đã từ chối xác nhận hoạt động mã hóa tập tin trên ổ đĩa di động.
- *Không hỗ trợ*. Chức năng mã hóa dữ liệu không khả dụng trên máy tính.

Xem trạng thái mã hóa

Để xem trạng thái mã hóa của dữ liệu máy tính:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, mở thư mục với tên của nhóm quản trị chứa máy tính liên quan.
3. Trong không gian làm việc, chọn thẻ **Các thiết bị**.

   Thẻ **Các thiết bị** trong không gian làm việc sẽ hiển thị thuộc tính của các máy tính trong nhóm quản trị được chọn.
4. Trên thẻ **Các thiết bị** trong không gian làm việc, vuốt thanh cuộn sang tận cùng bên phải.

   Cột **Trạng thái mã hóa** sẽ hiển thị trạng thái mã hóa của dữ liệu về các máy tính trong nhóm quản trị được chọn. Trạng thái này được tạo dựa trên thông tin về tình trạng mã hóa tập tin trên các ổ đĩa cục bộ của máy tính, tình trạng mã hóa của các ổ cứng máy tính, và tình trạng mã hóa các ổ đĩa di động được kết nối đến máy tính.

Xem số liệu mã hóa trong khung chi tiết của Kaspersky Security Center

Để xem trạng thái mã hóa trong khung chi tiết của Kaspersky Security Center:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Trong cây điều khiển, chọn nút **Máy chủ Quản trị – <Tên máy tính>**.
3. Trong không gian làm việc ở bên phải của cây Bảng điều khiển Quản trị, chọn thẻ **Thống kê**.
4. Tạo một trang mới với khung chi tiết chứa số liệu mã hóa dữ liệu. Để làm điều này:

a. Trên thẻ **Thống kê**, nhấn nút **Tùy chỉnh xem**.

Cửa sổ **Thuộc tính: Thống kê** sẽ được mở ra.

b. Trong cửa sổ **Thuộc tính: Thống kê**, nhấn nút **Thêm**.

Cửa sổ **Thuộc tính: Trang mới** sẽ được mở ra.

c. Trong mục **Tổng quát** của cửa sổ **Thuộc tính: Trang mới**, nhập tên trang.

d. Trong mục **Khung chi tiết**, nhấn nút **Thêm**.

Cửa sổ **Khung chi tiết mới** sẽ được mở ra.

e. Trong cửa sổ **Bảng điều khiển chi tiết mới** của nhóm **Trạng thái bảo vệ**, chọn mục **Mã hóa thiết bị**.

f. Nhấn **OK**.

Cửa sổ **Thuộc tính: Cửa sổ Kiểm soát Mã hóa** sẽ được mở ra.

g. Nếu cần, hãy sửa cấu hình khung chi tiết. Để làm điều này, sử dụng các mục **Xem** và **Các thiết bị** của cửa sổ **Thuộc tính: Cửa sổ Mã hóa Thiết bị**.

h. Nhấn **OK**.

i. Lặp lại các bước d – h của chỉ dẫn, sử dụng đề mục **Mã hóa ổ đĩa di động** trong mục **Trạng thái bảo vệ** của cửa sổ **Khung chi tiết mới**.

Khung chi tiết vừa được thêm sẽ xuất hiện trong danh sách **Khung chi tiết** của cửa sổ **Thuộc tính: Trang mới**.

j. Trong cửa sổ **Thuộc tính: Trang mới**, nhấn **OK**.

Tên của trang với khung chi tiết được tạo ở bước trước sẽ xuất hiện trong danh sách **Trang** của cửa sổ **Thuộc tính: Thống kê**.

k. Trong cửa sô **Thuộc tính: Thống kê**, nhấn nút **Đóng**.

5. Trên thẻ **Thống kê**, mở trang được tạo ở các bước trước của chỉ dẫn.

Khung chi tiết sẽ xuất hiện, hiển thị trạng thái mã hóa của các máy tính và ổ đĩa di động.

Xem lỗi mã hóa tập tin trên các ổ đĩa cục bộ trên máy tính

Để xem lỗi mã hóa tập tin trên các ổ đĩa cục bộ trên máy tính:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.

2. Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, mở thư mục với tên của nhóm quản trị chứa máy khách có danh sách lỗi mã hóa tập tin mà bạn muốn xem.

3. Trong không gian làm việc, chọn thẻ **Các thiết bị**.

4. Trên thẻ **Các thiết bị**, chọn tên của máy tính trong danh sách và nhấn phải chuột để mở menu ngữ cảnh.

5. Thực hiện một trong các thao tác sau:

- Trong menu ngữ cảnh của máy tính, chọn **Bảo vệ**.
- Trong menu ngữ cảnh của máy tính, chọn **Thuộc tính**. Trong cửa sổ **Thuộc tính: <tên máy tính>**, chọn mục **Bảo vệ**.

6. Trong mục **Bảo vệ** của cửa sổ **Thuộc tính: <tên máy tính>**, nhấn vào liên kết**Xem danh sách các lỗi mã hóa dữ liệu** để mở cửa sổ **Lỗi mã hóa dữ liệu**.

   Cửa sổ này sẽ hiển thị chi tiết các lỗi mã hóa tập tin trên các ổ đĩa cục bộ trên máy tính. Khi một lỗi được sửa, Kaspersky Security Center sẽ xóa chi tiết của lỗi đó khỏi cửa sổ **Lỗi mã hóa dữ liệu**.

Xem báo cáo mã hóa dữ liệu

Để xem báo cáo mã hóa dữ liệu:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Trong nút **Máy chủ Quản trị** của cây Bảng điều khiển Quản trị, chọn thẻ **Báo cáo**.
3. Nhấn nút **Tạo mẫu báo cáo**.

   Trình hướng dẫn Mẫu Báo cáo sẽ được bắt đầu.
4. Làm theo chỉ dẫn của Trình hướng dẫn Mẫu Báo cáo. Trong cửa sổ **Chọn loại mẫu báo cáo** trong mục **Khác**, chọn một trong các đề mục sau:
   - **Báo cáo trạng thái mã hóa của thiết bị được quản lý**.
   - **Báo cáo mã hóa dữ liệu trên thiết bị được lưu trữ**.
   - **Báo cáo lỗi mã hóa**.
   - **Báo cáo bị chặn truy cập đến các tập tin được mã hóa**.

   Sau khi bạn đã hoàn tất với Trình hướng dẫn Mẫu Báo cáo Mới, một mẫu báo cáo mới sẽ xuất hiện trong bảng trên thẻ **Báo cáo**.
5. Chọn mẫu báo cáo được tạo ở các bước trước của chỉ dẫn.

Tiến trình tạo báo cáo sẽ được bắt đầu. Báo cáo sẽ được hiển thị trong một cửa sổ mới.

Quản lý các tập tin được mã hóa với chức năng mã hóa tập tin hạn chế

Khi chính sách Kaspersky Security Center được áp dụng và tập tin sau đó được mã hóa, Kaspersky Endpoint Security sẽ được nhận một khóa mã hóa để truy cập trực tiếp vào các tập tin được mã hóa. Sử dụng khóa mã hóa này, một người dùng sử dụng bất kỳ tài khoản người dùng Windows nào đang hoạt động trong quá trình mã hóa tập tin cũng có thể truy cập trực tiếp vào các tập tin được mã hóa. Người dùng sử dụng các tài khoản Windows không hoạt động trong quá trình mã hóa tập tin phải kết nối đến Kaspersky Security Center để có thể truy cập các tập tin được mã hóa.

Các tập tin được mã hóa có thể không được truy cập trong các tình huống sau:

- Máy tính của người dùng chứa các khóa mã hóa, nhưng không có kết nối nào với Kaspersky Security Center để quản lý chúng. Trong trường hợp này, người dùng phải yêu cầu truy cập đến các tập tin được mã hóa từ quản trị viên mạng LAN.

  Nếu không tồn tại truy cập đến Kaspersky Security Center, bạn phải:

  - yêu cầu một khóa truy cập để truy cập các tập tin được mã hóa trên ổ cứng của máy tính;
  - để truy cập các tập tin được mã hóa có trên ổ đĩa di động, bạn cần yêu cầu các khóa truy cập riêng biệt cho các tập tin được mã hóa trên mỗi ổ đĩa di động.

- Các thành phần mã hóa bị xóa khỏi máy tính của người dùng. Trong trường hợp này, người dùng có thể mở các tập tin được mã hóa trên các ổ đĩa cục bộ và ổ đĩa di động, nhưng nội dung của các tập tin đó sẽ xuất hiện dưới dạng mã hóa.

  Người dùng có thể làm việc với các tập tin được mã hóa trong các trường hợp sau đây:

  - Các tập tin được đặt trong các gói mã hóa được tạo trên một máy tính có cài đặt Kaspersky Endpoint Security.
  - Các tập tin được lưu trữ trên một ổ đĩa di động có cho phép chế độ lưu động.

Truy cập các tập tin được mã hóa mà không kết nối đến Kaspersky Security Center

Các chỉ dẫn này dành cho người sử dụng của máy khách có cài đặt Kaspersky Endpoint Security.

Để truy cập các tập tin được mã hóa mà không kết nối đến Kaspersky Security Center:

1. Thực hiện truy cập đến tập tin được mã hóa mà bạn cần.

   Nếu không có kết nối nào với Kaspersky Security Center khi bạn cố gắng truy cập một tập tin được lưu trữ trên một ổ đĩa cục bộ của máy tính, Kaspersky Endpoint Security sẽ tạo một tập tin với yêu cầu truy cập tất cả các tập tin được mã hóa có trên ổ đĩa cục bộ của máy tính. Nếu bạn cố gắng truy cập một tập tin được lưu trữ trên một ổ đĩa di động, Kaspersky Endpoint Security sẽ tạo một tập tin với yêu cầu truy cập tất cả các tập tin được mã hóa có trên ổ đĩa di động đó. Cửa sổ **Truy cập tập tin bị chặn** sẽ được mở ra.

2. Gửi tập tin chứa yêu cầu truy cập đến tập tin được mã hóa đến cho quản trị viên mạng máy tính cục bộ. Để làm điều này, thực hiện một trong các hành động sau:

   - Để email tập tin yêu cầu truy cập các tập tin được mã hóa đến quản trị viên mạng máy tính cục bộ, nhấn nút **Gửi thư điện tử**
   - Để lưu tập tin yêu cầu truy cập các tập tin được mã hóa và gửi nó đến quản trị viên mạng LAN bằng một phương thức khác, nhấn nút **Lưu**.

3. Nhận tập tin khóa để truy cập các tập tin được mã hóa đã được tạo và cung cấp cho bạn bởi quản trị viên mạng máy tính cục bộ.

4. Kích hoạt khóa để truy cập các tập tin được mã hóa bằng một trong những cách sau đây:

   - Trong bất kỳ trình quản lý tập tin nào, chọn tập tin khóa để truy cập các tập tin được mã hóa. Nhấn đúp chuột để mở nó.

- Làm các bước sau:

  a. Mở cửa sổ chính của Kaspersky Endpoint Security.

  b. Nhấn nút .

  Việc này sẽ mở ra cửa sổ **Sự kiện**.

  c. Chọn thẻ **Trạng thái truy cập đến tập tin và thiết bị**.

  Thẻ này hiển thị một danh sách tất cả các yêu cầu truy cập các tập tin được mã hóa.

  d. Chọn yêu cầu mà qua đó bạn đã nhận tập tin khóa để truy cập các tập tin được mã hóa.

  e. Để nạp tập tin khóa được cung cấp và truy cập các tập tin được mã hóa, nhấn nút **Duyệt**.

  Hộp thoại **Lựa chọn tập tin khóa truy cập** tiêu chuẩn của Microsoft Windows sẽ được mở ra.

  f. Trong cửa sổ **Lựa chọn tập tin khóa truy cập** tiêu chuẩn của Microsoft Windows, chọn tập tin được quản trị viên cung cấp với phần mở rộng .kesdr và tên khớp với tên của tập tin yêu cầu truy cập.

  g. Nhấn nút **Mở**.

  h. Trong cửa sổ **Sự kiện**, nhấn **OK**.

Nếu một tập tin với yêu cầu truy cập các tập tin được mã hóa được tạo trong nỗ lực để truy cập vào một tập tin được lưu trữ trên một ổ đĩa cục bộ của máy tính, Kaspersky Endpoint Security sẽ cho phép truy cập đến tất cả các tập tin được mã hóa có trên ổ đĩa cục bộ của máy tính. Nếu một tập tin yêu cầu truy cập các tập tin được mã hóa được tạo trong nỗ lực truy cập một tập tin được lưu trữ trên một ổ đĩa di động, Kaspersky Endpoint Security sẽ cho phép người dùng truy cập đến tất cả các tập tin được mã hóa có trên ổ đĩa di động đó. Để truy cập các tập tin được lưu trữ trên các ổ đĩa di động khác, bạn phải nhận được một tập tin khóa truy cập riêng biệt cho mỗi ổ đĩa di động.

Cho phép người dùng truy cập đến các tập tin được mã hóa mà không kết nối đến Kaspersky Security Center

Để cho phép người dùng truy cập đến các tập tin được mã hóa mà không kết nối đến Kaspersky Security Center:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, mở thư mục với tên của nhóm quản trị chứa máy tính của người dùng yêu cầu truy cập đến các tập tin được mã hóa.
3. Trong không gian làm việc, chọn thẻ **Các thiết bị**.
4. Trên thẻ **Các thiết bị**, chọn máy tính của người dùng yêu cầu truy cập đến các tập tin được mã hóa và nhấn phải chuột để mở ra menu ngữ cảnh.
5. Trong menu ngữ cảnh, chọn **Cấp quyền truy cập vào thiết bị và các dữ liệu ở chế độ ngoại tuyến**.

   Cửa sổ **Cấp quyền truy cập vào thiết bị và các dữ liệu ở chế độ ngoại tuyến** sẽ được mở ra.
6. Trong cửa sổ **Cấp quyền truy cập vào thiết bị và các dữ liệu ở chế độ ngoại tuyến**, chọn thẻ **Mã hóa**.

7. Trên thẻ **Mã hóa**, nhấn nút **Duyệt**.

   Hộp thoại **Lựa chọn tập tin yêu cầu truy cập** tiêu chuẩn của Microsoft Windows sẽ được mở ra.

8. Trong cửa sổ **Lựa chọn tập tin yêu cầu truy cập**, nhập đường dẫn đến tập tin yêu cầu được nhận từ người dùng, và nhấn nút **Mở**.

   Kaspersky Security Center sẽ tạo một tập tin khóa để truy cập các tập tin được mã hóa này. Chi tiết của yêu cầu của người dùng sẽ được hiển thị trên thẻ **Mã hóa**.

9. Thực hiện một trong các thao tác sau:

   - Để email tập tin khóa truy cập vừa được tạo đến người dùng, nhấn nút **Gửi thư điện tử**.
   - Để lưu lại tập tin khóa truy cập cho các tập tin được mã hóa và gửi nó đến người dùng bằng một phương thức khác, nhấn nút **Lưu**.

Sửa mẫu thông điệp truy cập tập tin được mã hóa

Để sửa mẫu thông điệp truy cập tập tin được mã hóa:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, mở thư mục với tên của nhóm quản trị mà bạn muốn sửa mẫu thông điệp yêu cầu truy cập tập tin được mã hóa.
3. Trong không gian làm việc, chọn thẻ **Chính sách**.
4. Chọn chính sách cần thiết.
5. Mở cửa sổ **Thuộc tính: <Tên chính sách>** sử dụng một trong những phương pháp sau đây:

   - Trong menu ngữ cảnh của chính sách, chọn **Thuộc tính**.
   - Nhấn vào liên kết **Thiết lập chính sách** được đặt ở phần bên phải của không gian làm việc của Bảng điều khiển Quản trị.

6. Trong mục **Mã hóa dữ liệu**, chọn mục con **Cấu hình mã hóa chung**.
7. Trong mục **Mẫu**, chọn nút **Mẫu**.

   Cửa sổ **Mẫu** sẽ được mở ra.

8. Làm các bước sau:

   - Nếu bạn muốn sửa mẫu thông điệp của người dùng, chọn thẻ **Thông điệp của người dùng**. Cửa sổ **Truy cập tập tin bị từ chối** sẽ được mở ra khi người dùng cố gắng truy cập một tập tin được mã hóa nếu không có khóa khả dụng nào trên máy tính để truy cập vào các tập tin được mã hóa. Nhấn nút **Gửi thư điện tử** trong cửa sổ **Truy cập tập tin bị từ chối** để tự động tạo một thông điệp người dùng. Thông điệp này sẽ được gửi đến quản trị viên mạng LAN doanh nghiệp cùng với tập tin yêu cầu truy cập đến các tập tin được mã hóa.
   - Nếu bạn muốn sửa mẫu thông điệp quản trị viên, chọn thẻ **Thông điệp của người quản trị**. Thông điệp này sẽ tự động được tạo khi nút **Gửi thư điện tử** được nhấn trong cửa sổ **Cấp quyền truy cập đến các tập tin được mã hóa** và được gửi đến người dùng sau khi người dùng được cấp quyền truy cập đến các tập tin được mã hóa.

9. Sửa mẫu thông điệp.

   Bạn có thể sử dụng nút **Mặc định** và danh sách thả xuống **Biến số**.

10. Nhấn **OK**.

11. Để lưu thay đổi của bạn, trong cửa sổ **Thuộc tính: <Tên chính sách>**, nhấn **OK**.

Làm việc với các thiết bị được mã hóa khi không có truy cập đến chúng

Nhận quyền truy cập đến các thiết bị được mã hóa

Một người dùng sẽ cần yêu cầu truy cập đến các thiết bị được mã hóa trong các trường hợp sau:

- Một ổ cứng được mã hóa trên một máy tính khác.
- Khóa mã hóa cho thiết bị không có trên máy tính (ví dụ, ở lần đầu tiên truy cập ổ đĩa di động được mã hóa trên máy tính), và máy tính không được kết nối đến Kaspersky Security Center.

  Sau khi người dùng đã áp dụng khóa truy cập đến thiết bị mã hóa, Kaspersky Endpoint Security sẽ lưu khóa mã hóa trên máy tính của người dùng và cho phép truy cập đến thiết bị này ở các lần truy cập sau kể cả khi không có kết nối nào đến Kaspersky Security Center.

Quyền truy cập đến các thiết bị được mã hóa có thể được nhận như sau:

1. Người dùng sử dụng giao diện ứng dụng Kaspersky Endpoint Security để tạo một tập tin yêu cầu truy cập với phần mở rộng kesdc và gửi nó đến quản trị viên mạng LAN doanh nghiệp.
2. Quản trị viên sử dụng Bảng Điều khiển Quản trị Kaspersky Security Center để tạo một tập tin yêu cầu truy cập với phần mở rộng kesdr và gửi nó đến người dùng.
3. Người dùng áp dụng khóa truy cập.

Khôi phục dữ liệu trên các thiết bị được mã hóa

Một người dùng có thể sử dụng Tiện ích khôi phục thiết bị mã hóa (sau đây được gọi là Tiện ích Khôi phục) để làm việc với các thiết bị được mã hóa. Việc này có thể là cần thiết trong các trường hợp sau:

- Thủ tục sử dụng một khóa truy cập để nhận quyền truy cập đã không thành công.
- Các thành phần mã hóa không được cài đặt trên máy tính có thiết bị được mã hóa.

Dữ liệu cần thiết để khôi phục truy cập đến các thiết bị được mã hóa sử dụng Tiện ích Khôi phục đã nằm trong bộ nhớ của máy tính người dùng dưới dạng không mã hóa trong một thời gian nhất định. Để giảm thiểu nguy cơ truy cập trái phép đến các dữ liệu này, bạn chỉ nên khôi phục truy cập đến các thiết bị được mã hóa trên các máy tính được tin tưởng.

Dữ liệu trên các thiết bị được mã hóa có thể được khôi phục như sau:

1. Người dùng sử dụng Tiện ích Khôi phục để tạo một tập tin yêu cầu truy cập với phần mở rộng fdertc và gửi nó đến quản trị viên mạng LAN doanh nghiệp.

2. Quản trị viên sử dụng Bảng Điều khiển Quản trị Kaspersky Security Center để tạo một tập tin yêu cầu truy cập với phần mở rộng fdertr và gửi nó đến người dùng.

3. Người dùng áp dụng khóa truy cập.

Để khôi phục dữ liệu trên các ổ cứng hệ thống được mã hóa, người dùng cũng có thể nhập thông tin tài khoản Authentication Agent trong Tiện ích Khôi phục. Nếu siêu dữ liệu của tài khoản Authentication Agent đã bị hư hỏng, người dùng sẽ phải hoàn tất thủ tục khôi phục sử dụng một tập tin yêu cầu truy cập.

Trước khi khôi phục dữ liệu trên các thiết bị được mã hóa, bạn nên hủy bỏ chính sách mã hóa của Kaspersky Security Center trên máy tính được thực hiện hoạt động này. Điều này sẽ ngăn ổ đĩa được mã hóa lại một lần nữa.

Nhận quyền truy cập đến các thiết bị được mã hóa thông qua giao diện của ứng dụng

Các chỉ dẫn này dành cho người sử dụng của máy khách có cài đặt Kaspersky Endpoint Security.

Để nhận quyền truy cập đến các thiết bị được mã hóa thông qua giao diện của ứng dụng:

1. Cố truy cập đến thiết bị được mã hóa mà bạn cần.

   Cửa sổ **Truy cập vào dữ liệu bị chặn** sẽ được mở ra.

2. Gửi tập tin yêu cầu truy cập với phần mở rộng kesdc đến quản trị viên mạng LAN doanh nghiệp cho thiết bị được mã hóa. Để làm điều này, thực hiện một trong các hành động sau:

   - Để email tập tin yêu cầu truy cập được tạo cho thiết bị được mã hóa đến quản trị viên mạng LAN doanh nghiệp, nhấn nút **Gửi thư điện tử**.

   - Để lưu tập tin yêu cầu truy cập vào thiết bị được mã hóa và gửi nó đến quản trị viên mạng LAN doanh nghiệp bằng một phương thức khác, nhấn nút **Lưu**.

   Nếu bạn đã đóng cửa sổ **Truy cập vào dữ liệu bị chặn** mà không lưu tập tin yêu cầu truy cập, hoặc không gửi nó đến quản trị viên mạng LAN doanh nghiệp, bạn có thể làm việc này bất cứ lúc nào trong cửa sổ **Sự kiện** trên thẻ **Trạng thái truy cập đến tập tin và thiết bị**. Để mở cửa sổ này, nhấn nút trong cửa sổ chính của ứng dụng.

3. Nhận và lưu tập tin khóa truy cập vào thiết bị được mã hóa đã được quản trị viên mạng LAN doanh nghiệp tạo và cung cấp đến bạn.

4. Sử dụng một trong các phương thức sau đây để áp dụng khóa truy cập cho việc truy cập vào thiết bị được mã hóa:

   - Trong bất kỳ trình quản lý tập tin nào, tìm tập tin khóa truy cập vào thiết bị được mã hóa và nhấn đúp để mở nó.

- Làm các bước sau:

  a. Mở cửa sổ chính của Kaspersky Endpoint Security.

  b. Nhấn nút để mở ra cửa sổ **Sự kiện**.

  c. Chọn thẻ **Trạng thái truy cập đến tập tin và thiết bị**.

  Thẻ này hiển thị một danh sách tất cả các yêu cầu truy cập các tập tin và thiết bị được mã hóa.

  d. Chọn yêu cầu mà qua đó bạn đã nhận tập tin khóa truy cập cho việc truy cập vào thiết bị được mã hóa.

  e. Để nạp tập tin khóa truy cập được cung cấp và truy cập thiết bị được mã hóa, nhấn nút **Duyệt**.

  Hộp thoại **Lựa chọn tập tin khóa truy cập** tiêu chuẩn của Microsoft Windows sẽ được mở ra.

  f. Trong cửa sổ **Lựa chọn tập tin khóa truy cập** tiêu chuẩn của Microsoft Windows, chọn tập tin được quản trị viên cung cấp với phần mở rộng kesdr và tên khớp với tên của tập tin yêu cầu truy cập tương ứng cho thiết bị được mã hóa.

  g. Nhấn nút **Mở**.

  h. Trong cửa sổ **Trạng thái truy cập đến tập tin và thiết bị**, nhấn **OK**.

Kết quả là, Kaspersky Endpoint Security sẽ cấp quyền truy cập đến thiết bị được mã hóa.

Cấp cho người dùng quyền truy cập đến các thiết bị được mã hóa

Để cấp cho người dùng quyền truy cập đến một thiết bị được mã hóa:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, mở thư mục với tên của nhóm quản trị chứa máy tính của người dùng yêu cầu truy cập đến thiết bị được mã hóa.
3. Trong không gian làm việc, chọn thẻ **Các thiết bị**.
4. Trên thẻ **Các thiết bị**, chọn máy tính của người dùng yêu cầu truy cập đến thiết bị được mã hóa và nhấn phải chuột để mở ra menu ngữ cảnh.
5. Trong menu ngữ cảnh, chọn **Cấp quyền truy cập vào thiết bị và các dữ liệu ở chế độ ngoại tuyến**.

   Cửa sổ **Cấp quyền truy cập vào thiết bị và các dữ liệu ở chế độ ngoại tuyến** sẽ được mở ra.
6. Trong cửa sổ **Cấp quyền truy cập vào thiết bị và các dữ liệu ở chế độ ngoại tuyến**, chọn thẻ **Mã hóa**.
7. Trên thẻ **Mã hóa**, nhấn nút **Duyệt**.

   Hộp thoại **Lựa chọn tập tin yêu cầu truy cập** tiêu chuẩn của Microsoft Windows sẽ được mở ra.
8. Trong cửa sổ **Lựa chọn tập tin yêu cầu truy cập**, nhập đường dẫn đến tập tin yêu cầu với phần mở rộng kesdc mà bạn đã nhận từ người dùng.
9. Nhấn nút **Mở**.

Kaspersky Security Center sẽ tạo một tập tin khóa truy cập vào thiết bị được mã hóa với phần mở rộng kesdr. Chi tiết của yêu cầu của người dùng sẽ được hiển thị trên thẻ **Mã hóa**.

10. Thực hiện một trong các thao tác sau:

    - Để email tập tin khóa truy cập vừa được tạo đến người dùng, nhấn nút **Gửi thư điện tử**.
    - Để lưu lại tập tin khóa truy cập cho thiết bị được mã hóa và gửi nó đến người dùng bằng một phương thức khác, nhấn nút **Lưu**.

Cung cấp cho người dùng một khóa khôi phục cho các ổ cứng được mã hóa với BitLocker

Để gửi đến một người dùng một khóa khôi phục cho ổ cứng hệ thống được mã hóa bởi BitLocker:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, mở thư mục với tên của nhóm quản trị chứa máy tính của người dùng yêu cầu truy cập đến ổ đĩa được mã hóa.
3. Trong không gian làm việc, chọn thẻ **Các thiết bị**.
4. Trên thẻ **Các thiết bị**, chọn máy tính của người dùng yêu cầu truy cập đến ổ đĩa di động được mã hóa.
5. Nhấn phải chuột để mở menu ngữ cảnh và chọn **Cấp quyền truy cập vào thiết bị và các dữ liệu ở chế độ ngoại tuyến**.

   Cửa sổ **Cấp quyền truy cập vào thiết bị và các dữ liệu ở chế độ ngoại tuyến** sẽ được mở ra.
6. Trong cửa sổ **Cấp quyền truy cập vào thiết bị và các dữ liệu ở chế độ ngoại tuyến**, chọn thẻ **Truy cập một ổ đĩa hệ thống được bảo vệ bởi BitLocker**.
7. Nhắc người dùng nhập ID khóa khôi phục được ghi trong cửa sổ nhập mật khẩu BitLocker, và so sánh nó với ID trong trường **ID khóa phục hồi**.

   Nếu các ID không khớp nhau, khóa này sẽ không thể khôi phục truy cập đến ổ đĩa hệ thống được quy định. Hãy đảm bảo là tên của máy tính được chọn khớp với tên máy tính của người sử dụng.
8. Gửi đến người dùng khóa được ghi trong trường **Khóa phục hồi**.

Để gửi đến một người dùng một khóa khôi phục cho ổ cứng không phải ổ cứng hệ thống được mã hóa bởi BitLocker:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Trong cây Bảng điều khiển Quản trị, chọn thư mục **Bổ sung → Mã hóa và bảo vệ dữ liệu → Thiết bị được mã hóa**.

   Không gian làm việc sẽ hiển thị một danh sách thiết bị được mã hóa.
3. Trong không gian làm việc, chọn thiết bị được mã hóa mà bạn muốn khôi phục truy cập.

4. Nhấn phải chuột để gọi menu ngữ cảnh và chọn **Nhận khóa truy cập đến thiết bị được mã hóa cụ thể**.

   Việc này sẽ mở ra cửa sổ **Khôi phục truy cập đến một ổ đĩa được mã hóa với BitLocker**.

5. Nhắc người dùng nhập ID khóa khôi phục được ghi trong cửa sổ nhập mật khẩu BitLocker, và so sánh nó với ID trong trường **ID khóa phục hồi**.

   Nếu các ID không khớp nhau, khóa này sẽ không thể khôi phục truy cập đến ổ đĩa được quy định. Hãy đảm bảo là tên của máy tính được chọn khớp với tên máy tính của người sử dụng.

6. Gửi đến người dùng khóa được ghi trong trường **Khóa phục hồi**.

Tạo tập tin thực thi của Tiện ích Khôi phục

Các chỉ dẫn này dành cho người sử dụng của máy khách có cài đặt Kaspersky Endpoint Security.

Để tạo tập tin thực thi của Tiện ích Khôi phục:

1. Mở cửa sổ chính của ứng dụng.
2. Nhấn vào nút ở góc dưới trái của cửa sổ chính của ứng dụng để mở cửa sổ **Hỗ trợ**.
3. Trong cửa sổ **Hỗ trợ**, nhấn nút **Khôi phục thiết bị mã hóa**.

   Tiện ích Khôi phục thiết bị được mã hóa sẽ được bắt đầu.

4. Nhấn nút **Tạo tiện ích khôi phục độc lập** trong cửa sổ Tiện ích Khôi phục.

   Cửa sổ **Tạo tiện ích khôi phục độc lập** sẽ được mở ra.

5. Trong cửa sổ **Lưu vào**, nhập thủ công đường dẫn đến thư mục để lưu tập tin thực thi của Tiện ích Khôi phục, hoặc nhấn nút **Duyệt**.
6. Nhấn **OK** trong cửa sổ **Tạo tiện ích khôi phục độc lập**.

   Tập tin thực thi của Tiện ích Khôi phục (fdert.exe) sẽ được lưu trong thư mục được chọn.

Khôi phục dữ liệu trên các thiết bị được mã hóa sử dụng Tiện ích Khôi phục

Các chỉ dẫn này dành cho người sử dụng của máy khách có cài đặt Kaspersky Endpoint Security.

Để khôi phục truy cập đến thiết bị được mã hóa sử dụng Tiện ích Khôi phục:

1. Chạy Tiện ích Khôi phục bằng một trong các cách sau:

   - Nhấn nút trong cửa sổ chính của Kaspersky Endpoint Security để mở cửa sổ **Hỗ trợ** và nhấn nút **Khôi phục thiết bị mã hóa**.

- Chạy tập tin thực thi fdert.exe của Tiện ích Khôi phục. Tập tin này được tạo bởi Kaspersky Endpoint Security.

2. Trong cửa sổ Tiện ích Khôi phục, từ danh sách thả xuống **Lựa chọn thiết bị**, chọn một thiết bị được mã hóa mà bạn muốn khôi phục quyền truy cập vào đó.

3. Nhấn nút **Quét** để cho phép thiết bị xác định hành động nào nên được thực thi đối với thiết bị: liệu nó nên được mở khóa hay giải mã.

   Nếu máy tính có thể truy cập chức năng mã hóa của Kaspersky Endpoint Security, Tiện ích Khôi phục sẽ nhắc bạn mở khóa thiết bị. Tuy việc mở khóa thiết bị không giải mã cho nó, nhưng thiết bị có thể được truy cập trực tiếp khi được mở khóa. Nếu máy tính không thể truy cập chức năng mã hóa của Kaspersky Endpoint Security, Tiện ích Khôi phục sẽ nhắc bạn giải mã thiết bị.

4. Nhấn nút **Sửa chữa MBR** nếu tiến trình chẩn đoán ổ cứng hệ thống được mã hóa trả về thông điệp sự cố liên quan đến bản ghi khởi động tổng (MBR) của thiết bị.

   Việc sửa bản ghi khởi động tổng của thiết bị có thể tăng tốc tiến trình thu thập thông tin cần thiết để mở khóa hoặc giải mã thiết bị.

5. Nhấn nút **Mở khóa** hay **Giải mã** tùy thuộc vào kết quả của chẩn đoán.

   Cửa sổ **Thiết lập mở khóa thiết bị** hoặc **Thiết lập giải mã thiết bị** sẽ được mở ra.

6. Nếu bạn muốn khôi phục dữ liệu sử dụng một tài khoản Authentication Agent:

   a. Chọn mục **Sử dụng tham số tài khoản Authentication Agent**.

   b. Trong trường **Tên** và **Mật khẩu**, nhập thông tin đăng nhập cho tài khoản Authentication Agent.

   Phương thức này chỉ có thể được sử dụng khi khôi phục dữ liệu trên một ổ cứng hệ thống. Nếu ổ cứng hệ thống bị hư hỏng và dữ liệu tài khoản Authentication Agent bị mất, bạn sẽ phải nhận một khóa truy cập từ quản trị viên mạng LAN doanh nghiệp để có thể khôi phục dữ liệu trên một thiết bị được mã hóa.

7. Nếu bạn muốn sử dụng một khóa truy cập để khôi phục dữ liệu:

   a. Chọn mục **Chỉ định khóa truy cập thiết bị theo cách thủ công**.

   b. Nhấn nút **Nhận khóa truy cập**.

   c. Cửa sổ **Nhận khóa truy cập thiết bị** sẽ được mở ra.

   d. Nhấn nút **Lưu** và chọn thư mục để lưu tập tin yêu cầu truy cập với phần mở rộng fdertc.

   e. Gửi tập tin yêu cầu truy cập đến quản trị viên mạng LAN doanh nghiệp.

   > Không đóng cửa sổ **Nhận khóa truy cập thiết bị** cho đến khi bạn đã nhận được khóa truy cập. Khi cửa sổ này được mở lại, bạn sẽ không thể áp dụng khóa truy cập đã được quản trị viên tạo trước đó.

   f. Nhận và lưu tập tin khóa truy cập được quản trị viên mạng LAN doanh nghiệp tạo và cung cấp đến bạn.

   g. Nhấn nút **Tải** và chọn tập tin khóa truy cập với phần mở rộng fdertr trong cửa sổ được mở ra.

8. Nếu bạn đang giải mã một thiết bị, bạn cũng phải nhập các thiết lập giải mã khác trong cửa sổ **Cấu hình giải mã thiết bị**. Để làm điều này:

   - Chọn khu vực để giải mã:

     - Nếu bạn muốn giải mã toàn bộ thiết bị, chọn mục **Giải mã toàn bộ thiết bị**.

     - Nếu bạn chỉ muốn giải mã một phần dữ liệu trên một thiết bị, chọn mục **Giải mã khu vực riêng của thiết bị** và sử dụng các trường **Bắt đầu** và **Kết thúc** để quy định ranh giới khu vực được giải mã.

   - Chọn địa điểm để ghi dữ liệu được giải mã:

     - Nếu bạn muốn dữ liệu trên thiết bị gốc được ghi đè bởi dữ liệu được mã hóa, hãy xóa hộp kiểm **Lưu dữ liệu vào tập tin sau khi giải mã**.

     - Nếu bạn muốn lưu dữ liệu được giải mã tách riêng khỏi dữ liệu mã hóa gốc, chọn hộp kiểm **Lưu dữ liệu vào tập tin sau khi giải mã** và sử dụng nút **Duyệt** để quy định đường dẫn đến nơi lưu dữ liệu.

9. Nhấn **OK**.

Tiến trình mở khóa / giải mã thiết bị sẽ được bắt đầu.

Đáp lại yêu cầu của người dùng để khôi phục dữ liệu trên các thiết bị được mã hóa

Để tạo một tập tin khóa cho việc truy cập một thiết bị được mã hóa và cung cấp nó đến người dùng:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.

2. Trong cây Bảng điều khiển Quản trị, chọn thư mục **Bổ sung → Mã hóa và bảo vệ dữ liệu → Thiết bị được mã hóa**.

3. Trong không gian làm việc, chọn thiết bị được mã hóa mà bạn muốn tạo một tập tin khóa truy cập, và trong menu ngữ cảnh của thiết bị đó chọn **Nhận khóa truy cập đến thiết bị mã hóa được chọn**.

   > Nếu bạn không chắc chắn tập tin yêu cầu truy cập được tạo cho máy tính nào, trong cây Bảng điều khiển Quản trị, chọn thư mục **Bổ sung → Mã hóa và bảo vệ dữ liệu** và trong không gian làm việc, nhấn vào liên kết **Nhận khóa mã hóa của thiết bị**.

   Cửa sổ **Cho phép truy cập đến thiết bị** sẽ được mở ra.

4. Chọn thuật toán mã hóa được sử dụng. Để làm điều này, chọn một trong các phương án sau:

   - **AES256**, nếu Kaspersky Endpoint Security được cài đặt từ một gói phân phối nằm trong thư mục aes256 trên máy tính đã mã hóa thiết bị;

   - **AES56**, nếu Kaspersky Endpoint Security được cài đặt từ một gói phân phối nằm trong thư mục aes56 trên máy tính đã mã hóa thiết bị;

5. Nhấn nút **Duyệt**.

   Hộp thoại **Lựa chọn tập tin yêu cầu truy cập** tiêu chuẩn của Microsoft Windows sẽ được mở ra.

6. Trong cửa sổ **Lựa chọn tập tin yêu cầu truy cập**, nhập đường dẫn đến tập tin yêu cầu với phần mở rộng fdertc mà bạn đã nhận từ người dùng.

7. Nhấn nút **Mở**.

   Kaspersky Security Center sẽ tạo một tập tin khóa truy cập với phần mở rộng fdertr để truy cập thiết bị được mã hóa này.

8. Thực hiện một trong các thao tác sau:

   - Để email tập tin khóa truy cập vừa được tạo đến người dùng, nhấn nút **Gửi thư điện tử**.
   - Để lưu lại tập tin khóa truy cập cho thiết bị được mã hóa và gửi nó đến người dùng bằng một phương thức khác, nhấn nút **Lưu**.

Khôi phục truy cập đến dữ liệu được mã hóa sau khi hỏng hệ điều hành

Bạn chỉ có thể khôi phục truy cập đến dữ liệu sau khi hỏng hệ điều hành cho mã hóa mức độ tập tin (FLE). Bạn không thể khôi phục quyền truy cập đến dữ liệu nếu sử dụng mã hóa toàn bộ ổ đĩa (FDE).

Để khôi phục truy cập đến dữ liệu được mã hóa sau khi hỏng hệ điều hành:

1. Cài đặt lại hệ điều hành mà không format ổ cứng.

2. Cài đặt Kaspersky Endpoint Security.

3. Thiết lập một kết nối giữa máy tính và Máy chủ Quản trị Kaspersky Security Center đã kiểm soát máy tính trong quá trình mã hóa dữ liệu.

Quyền đến dữ liệu được mã hóa sẽ được cấp theo cùng các điều kiện đã được áp dụng trước khi hỏng hệ điều hành.

Tạo một rescue disk cho hệ điều hành

Rescue disk cho hệ điều hành có thể rất hữu ích khi một ổ cứng được mã hóa không thể được truy cập vì một lý do nào đó, và hệ điều hành không thể được nạp.

Bạn có thể tải hình ảnh của hệ điều hành Windows sử dụng rescue disk và khôi phục truy cập đến ổ cứng được mã hóa sử dụng Tiện ích Khôi phục được bao gồm trong hình ảnh hệ điều hành.

Để tạo một rescue disk cho hệ điều hành:

1. Tạo một tập tin thực thi cho Tiện ích Khôi phục Thiết bị được Mã hóa.

2. Tạo một hình ảnh tùy chỉnh của môi trường tiền khởi động Windows. Trong khi tạo một hình ảnh tùy chỉnh của môi trường tiền khởi động Windows, bổ sung tập tin thực thi của Tiện ích Khôi phục vào hình ảnh.

3. Lưu hình ảnh tùy chỉnh của môi trường tiền cài đặt Windows vào ổ khởi động được như đĩa CD hoặc ổ đĩa di động.

Tham khảo các tập tin trợ giúp của Microsoft để được hướng dẫn cách tạo một hình ảnh tùy chỉnh của môi trường tiền khởi động Windows (ví dụ, trong tài nguyên của Microsoft TechNet).

Bảo vệ Mạng

Phần này chứa thông tin về giám sát lưu lượng mạng và hướng dẫn cách để thiết lập cấu hình các cổng mạng bị giám sát.

Thông tin về Bảo vệ Mạng

Trong quá trình hoạt động của Kaspersky Endpoint Security, các thành phần như Chống virus cho thư điện tử, Chống virus cho web và Chống virus cho tin nhắn sẽ giám sát các dòng dữ liệu được truyền tải qua các giao thức cụ thể và được truyền tải thông qua các cổng TCP và UDP mở cụ thể trên máy tính của bạn. Ví dụ, Chống virus cho thư điện tử sẽ quét dữ liệu được truyền tải qua SMTP, còn Chống virus cho web sẽ quét dữ liệu được truyền tải qua HTTP và FTP.

Kaspersky Endpoint Security sẽ chia các cổng TCP và UDP của hệ điều hành thành nhiều nhóm tùy thuộc vào khả năng chúng bị xâm nhập. Một số cổng mạng được dành riêng cho các dịch vụ có thể có lỗ hổng bảo mật. Bạn được khuyến nghị giám sát kỹ lưỡng các cổng đó bởi nguy cơ chúng bị tấn công là cao hơn. Nếu bạn sử dụng các dịch vụ không tiêu chuẩn, dựa trên các cổng mạng không tiêu chuẩn, các cổng mạng này cũng có thể bị nhắm đến bởi một máy tính thực hiện tấn công. Bạn có thể quy định một danh sách các cổng mạng và một danh sách các ứng dụng yêu cầu truy cập mạng. Những cổng và ứng dụng này sau đó sẽ nhận được sự chú ý đặc biệt của các thành phần Chống virus cho thư điện tử, Chống virus cho web và Chống virus cho tin nhắn khi chúng giám sát lưu lượng mạng.

Thiết lập cấu hình giám sát lưu lượng mạng

Bạn có thể thực hiện các hành động sau để thiết lập cấu hình giám sát lưu lượng mạng:

- Bật tính năng giám sát tất cả các cổng mạng.
- Tạo một danh sách các cổng mạng bị giám sát.
- Tạo một danh sách ứng dụng được giám sát tất cả các cổng mạng.

Bật tính năng giám sát tất cả các cổng mạng

Để bật tính năng giám sát tất cả các cổng mạng:

1. Mở cửa sổ cấu hình ứng dụng.
2. Ở phần bên trái của cửa sổ, chọn mục **Bảo vệ Chống virus**.
   Cấu hình bảo vệ chống virus sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Trong mục **Các cổng được giám sát**, chọn **Giám sát tất cả các cổng mạng**.
4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Tạo một danh sách các cổng mạng bị giám sát

Để tạo một danh sách các cổng mạng bị giám sát:

1. Mở cửa sổ cấu hình ứng dụng.
2. Ở phần bên trái của cửa sổ, chọn mục **Bảo vệ Chống virus**.

   Cấu hình bảo vệ chống virus sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Trong mục **Các cổng được giám sát**, chọn **Chỉ giám sát các cổng được chọn**.
4. Nhấn nút **Cấu hình**.

   Cửa sổ **Các cổng mạng** sẽ được mở ra. Cửa sổ **Các cổng mạng** hiển thị một danh sách các cổng mạng thường được sử dụng để truyền tải email và lưu lượng mạng. Danh sách các cổng mạng này được bao gồm trong gói Kaspersky Endpoint Security.
5. Trong danh sách các cổng mạng, làm thao tác sau:

   - Chọn hộp kiểm đối diện các cổng mạng mà bạn muốn bao gồm trong danh sách các cổng mạng bị giám sát.

     Theo mặc định, các hộp kiểm đối diện tất cả các cổng mạng được liệt kê trong cửa sổ **Các cổng mạng** đều được chọn.
   - Xóa hộp kiểm đối diện các cổng mạng mà bạn muốn loại trừ khỏi danh sách các cổng mạng bị giám sát.
6. Nếu cổng mạng không được hiển thị trong danh sách các cổng mạng, hãy thêm nó bằng cách:

   a. Trong danh sách các cổng mạng, nhấn vào liên kết **Thêm** để mở ra cửa sổ **Cổng mạng**.

   b. Nhập số hiệu cổng mạng vào trường **Cổng**.

   c. Nhập tên của cổng mạng vào trường **Mô tả**.

   d. Nhấn **OK**.

      Cửa sổ **Cổng mạng** sẽ được đóng lại. Cổng mạng vừa được thêm sẽ được hiển thị ở cuối danh sách các cổng mạng.
7. Trong cửa sổ **Các cổng mạng**, nhấn **OK**.
8. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Khi giao thức FTP chạy trong chế độ thụ động, kết nối có thể được thiết lập qua một cổng mạng ngẫu nhiên không được thêm vào danh sách các cổng mạng bị giám sát. Để bảo vệ những kết nối này, chọn hộp kiểm **Giám sát tất cả các cổng mạng** trong mục **Các cổng được giám sát** hoặc cấu hình việc giám sát tất cả các cổng của ứng dụng thiết lập kết nối FTP.

Tạo một danh sách ứng dụng được giám sát tất cả các cổng mạng

Bạn có thể tạo một danh sách ứng dụng sẽ được Kaspersky Endpoint Security giám sát tất cả các cổng mạng.

Chúng tôi khuyến nghị bạn bao gồm các ứng dụng nhận và truyền tải dữ liệu qua giao thức FTP trong danh sách ứng dụng sẽ được Kaspersky Endpoint Security giám sát tất cả các cổng mạng.

Để tạo một danh sách ứng dụng được giám sát tất cả các cổng mạng:

1. Mở cửa sổ cấu hình ứng dụng.
2. Ở phần bên trái của cửa sổ, chọn mục **Bảo vệ Chống virus**.
   Cấu hình bảo vệ chống virus sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Trong mục **Các cổng được giám sát**, chọn **Chỉ giám sát các cổng được chọn**.
4. Nhấn nút **Cấu hình**.
   Cửa sổ **Các cổng mạng** sẽ được mở ra.
5. Chọn hộp kiểm **Theo dõi tất cả các cổng của những ứng dụng được chỉ định**.
6. Trong danh sách các ứng dụng dưới hộp kiểm **Theo dõi tất cả các cổng của những ứng dụng được chỉ định**, làm thao tác sau:
   - Chọn hộp kiểm cạnh tên của các ứng dụng mà bạn muốn giám sát tất cả các cổng mạng.
     Theo mặc định, các hộp kiểm cạnh tất cả các ứng dụng được liệt kê trong cửa sổ **Các cổng mạng** đều được chọn.
   - Xóa hộp kiểm cạnh tên của các ứng dụng mà bạn không muốn giám sát tất cả các cổng mạng.
7. Nếu một ứng dụng không được bao gồm trong danh sách ứng dụng, hãy bổ sung chúng bằng cách sau:
   a. Nhấn liên kết **Thêm** ở dưới danh sách ứng dụng và mở ra menu ngữ cảnh.
   b. Trong menu ngữ cảnh, chọn cách để thêm ứng dụng vào danh sách các ứng dụng:
      - Để chọn một ứng dụng từ danh sách các ứng dụng được cài đặt trên máy tính, chọn lệnh **Ứng dụng**. Cửa sổ **Lựa chọn ứng dụng** sẽ được mở ra, cho phép bạn quy định tên của ứng dụng.
      - Để nhập vị trí của tập tin thực thi của ứng dụng, chọn lệnh **Duyệt**. Cửa sổ **Mở** tiêu chuẩn trong Microsoft Windows sẽ được mở ra, cho phép bạn quy định tên của tập tin thực thi của ứng dụng.

      Cửa sổ **Ứng dụng** sẽ được mở ra sau khi bạn chọn ứng dụng.
   c. Trong trường **Tên**, hãy nhập tên cho ứng dụng được chọn.
   d. Nhấn **OK**.
      Cửa sổ **Ứng dụng** sẽ được đóng lại. Ứng dụng mà bạn vừa thêm vào sẽ xuất hiện ở cuối danh sách ứng dụng.
8. Trong cửa sổ **Các cổng mạng**, nhấn **OK**.
9. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Cập nhật cơ sở dữ liệu và các mô-đun phần mềm ứng dụng

Phần này chứa thông tin về việc cập nhật mô-đun ứng dụng và cơ sở dữ liệu (còn gọi là "cập nhật"), và hướng dẫn cách để thiết lập cấu hình cập nhật.

Thông tin về các bản cập nhật cơ sở dữ liệu và mô-đun ứng dụng

Việc cập nhật cơ sở dữ liệu và mô-đun ứng dụng của Kaspersky Endpoint Security đảm bảo tính năng bảo vệ mới nhất cho máy tính của bạn. Các virus và những loại phần mềm độc hại khác xuất hiện hàng ngày trên toàn thế giới. Cơ sở dữ liệu Kaspersky Endpoint Security chứa thông tin về những mối đe dọa và các cách để loại trừ chúng. Để phát hiện nhanh chóng các mối đe dọa, bạn được khuyến nghị cập nhật thường xuyên các cơ sở dữ liệu và mô-đun ứng dụng.

Việc cập nhật thường xuyên đòi hỏi một giấy phép còn hiệu lực. Nếu không có giấy phép hiện tại, bạn sẽ chỉ có thể thực hiện cập nhật một lần duy nhất.

Nguồn cập nhật chính của Kaspersky Endpoint Security là các máy chủ cập nhật Kaspersky.

Máy tính của bạn phải được kết nối đến Internet để có thể tải về gói cập nhật từ các máy chủ cập nhật của Kaspersky. Theo mặc định, các cấu hình kết nối Internet sẽ được xác định một cách tự động. Nếu bạn sử dụng một máy chủ proxy, bạn sẽ cần điều chỉnh thiết lập kết nối.

Trong khi thực hiện cập nhật, các đối tượng sau đây sẽ được tải về và cài đặt trên máy tính của bạn:

- Cơ sở dữ liệu Kaspersky Endpoint Security. Tính năng bảo vệ máy tính được cung cấp sử dụng các cơ sở dữ liệu chứa ký hiệu của các virus và các mối đe dọa khác, cũng như thông tin về các cách để vô hiệu hóa chúng. Các thành phần bảo vệ sử dụng thông tin này khi tìm kiếm và vô hiệu quá các tập tin bị nhiễm trên máy tính của bạn. Các cơ sở dữ liệu sẽ liên tục được cập nhật với hồ sơ các mối đe dọa mới, cũng như các biện pháp để loại trừ chúng. Bởi vậy, chúng tôi khuyến nghị bạn thường xuyên cập nhật cơ sở dữ liệu.

  Ngoài các cơ sở dữ liệu Kaspersky Endpoint Security, trình điều khiển mạng cho phép các thành phần của ứng dụng có thể theo dõi lưu lượng mạng cũng sẽ được cập nhật.

- Mô-đun ứng dụng. Ngoài các cơ sở dữ liệu của Kaspersky Endpoint Security, bạn cũng có thể cập nhật các mô-đun ứng dụng. Việc cập nhật các mô-đun ứng dụng sẽ khắc phục những lỗ hổng bảo mật trong Kaspersky Endpoint Security, bổ sung các chức năng mới, hoặc tăng cường các chức năng sẵn có.

Trong khi cập nhật, các mô-đun ứng dụng và cơ sở dữ liệu trên máy tính của bạn sẽ được so sánh với các phiên bản đã cập nhật tại nguồn cập nhật. Nếu cơ sở dữ liệu và các mô-đun ứng dụng hiện tại của bạn khác với các phiên bản cập nhật tương ứng, phần còn thiếu của bản cập nhật sẽ được cài đặt trên máy tính của bạn.

Các tập tin trợ giúp ngữ cảnh có thể được cập nhật cùng với các bản cập nhật mô-đun ứng dụng.

Nếu cơ sở dữ liệu đã lỗi thời, gói cập nhật có thể lớn hơn, và làm tăng lưu lượng Internet (lên đến vài chục MB).

Thông tin về trạng thái hiện tại của cơ sở dữ liệu Kaspersky Endpoint Security được hiển thị trong phần **Cập nhật** của mục **Tác vụ** trên thẻ **Bảo vệ và Kiểm soát** của cửa sổ chính của ứng dụng.

Thông tin về kết quả cập nhật và tất cả các sự kiện đã xảy ra trong quá trình thực thi tác vụ cập nhật được ghi lại trong báo cáo của Kaspersky Endpoint Security.

Thông tin về nguồn cập nhật

Nguồn cập nhật là một tài nguyên chứa các bản cập nhật cơ sở dữ liệu và mô-đun ứng dụng của Kaspersky Endpoint Security.

Nguồn cập nhật bao gồm máy chủ Kaspersky Security Center và Kaspersky, máyy chủ cập nhật của Kaspersky và các thư mục cục bộ hoặc thư mục mạng.

Thiết lập cấu hình cập nhật

Bạn có thể thực hiện các hành động sau để thiết lập cấu hình cập nhật:

- Bổ sung các nguồn cập nhật mới.

  Danh sách mặc định các nguồn cập nhật bao gồm máy chủ cập nhật của Kaspersky Security Center và Kaspersky. Bạn có thể thêm các nguồn cập nhật khác vào danh sách. Bạn có thể quy định các máy chủ HTTP/FTP và các thư mục được chia sẻ làm nguồn cập nhật.

  Nếu nhiều tài nguyên cùng được chọn làm nguồn cập nhật, Kaspersky Endpoint Security sẽ cố gắng kết nối đến từng tài nguyên một, bắt đầu từ đầu danh sách và thực hiện tác vụ cập nhật bằng cách truy hồi gói cập nhật từ nguồn khả dụng đầu tiên.

  > Nếu bạn đã chọn một tài nguyên ngoài mạng LAN làm nguồn cập nhật, bạn phải có một kết nối Internet để thực hiện cập nhật.

- Chọn khu vực đặt máy chủ cập nhật Kaspersky.

  Nếu bạn sử dụng các máy chủ cập nhật của Kaspersky làm nguồn cập nhật, bạn có thể chọn vị trí của máy chủ cập nhật Kaspersky được sử dụng để tải về gói cập nhật. Các máy chủ cập nhật Kaspersky được đặt ở nhiều quốc gia khác nhau. Việc sử dụng máy chủ cập nhật Kaspersky gần nhất giúp giảm thiểu thời gian dành cho việc truy hồi một gói cập nhật.

  Theo mặc định, ứng dụng sẽ sử dụng thông tin về khu vực hiện tại từ registry của hệ điều hành.

- Thiết lập việc cập nhật của Kaspersky Endpoint Security từ một thư mục được chia sẻ.

  Để tiết kiệm lưu lượng Internet, bạn có thể thiết lập các bản cập nhật Kaspersky Endpoint Security để máy tính trên mạng LAN của bạn nhận các bản cập nhật từ một thư mục chia sẻ. Để làm điều này, một máy tính trên mạng LAN của bạn sẽ nhận gói cập nhật mới nhất từ máy chủ Kaspersky Security Center hoặc máy chủ cập nhật Kaspersky, và sao chép gói cập nhật nhận được đến một thư mục được chia sẻ. Sau đó, các máy tính khác trên mạng LAN của bạn sẽ có thể nhận gói cập nhật từ thư mục chia sẻ này.

- Chọn chế độ chạy tác vụ cập nhật.

  Nếu không thể chạy tác vụ vì bất cứ lý do gì (ví dụ, máy tính đang tắt tại thời điểm đó), bạn có thể thiết lập tác vụ bị bỏ qua được tự động chạy lại ngay khi có thể.

Bạn có thể hoãn việc khởi động tác vụ cập nhật sau khi ứng dụng khởi động nếu chọn chế độ chạy tác vụ cập nhật **Theo lập lịch**, và nếu thời gian khởi động của Kaspersky Endpoint Security khớp với lịch khởi động tác vụ cập nhật. Tác vụ cập nhật chỉ có thể được chạy sau khoảng thời gian được quy định từ lúc khởi động Kaspersky Endpoint Security.

- Thiết lập tác vụ cập nhật để chạy theo quyền của một tài khoản người dùng khác.

Bổ sung một nguồn cập nhật

Để bổ sung một nguồn cập nhật:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Tác vụ được lập lịch**, chọn **Cập nhật**.
   Cấu hình Cập nhật Ứng dụng sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Trong mục **Chế độ chạy và nguồn cập nhật**, nhấn nút **Nguồn cập nhật**.
   Việc này sẽ mở ra thẻ **Nguồn** trong cửa sổ **Cập nhật**.
4. Trên thẻ **Nguồn**, nhấn nút **Thêm**.
   Cửa sổ **Lựa chọn nguồn cập nhật** sẽ được mở ra.
5. Trong cửa sổ **Lựa chọn nguồn cập nhật**, chọn một thư mục với gói cập nhật hoặc nhập đường dẫn đầy đủ đến thư mục trong trường **Nguồn**.
6. Nhấn **OK**.
7. Trong cửa sổ **Cập nhật**, nhấn **OK**.
8. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Chọn khu vực máy chủ cập nhật

Để chọn khu vực máy chủ cập nhật:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Tác vụ được lập lịch**, chọn **Cập nhật**.
   Cấu hình Cập nhật Ứng dụng sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Trong mục **Chế độ chạy và nguồn cập nhật**, nhấn nút **Nguồn cập nhật**.
   Việc này sẽ mở ra thẻ **Nguồn** trong cửa sổ **Cập nhật**.
4. Trên thẻ **Nguồn**, trong mục **Cấu hình khu vực**, chọn **Lựa chọn từ danh sách**.
5. Trong danh sách thả xuống, chọn quốc gia gần vị trí hiện tại của bạn nhất.
6. Nhấn **OK**.

7. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Thiết lập cập nhật từ một thư mục được chia sẻ

Thiết lập việc cập nhật của Kaspersky Endpoint Security từ một thư mục được chia sẻ bao gồm các bước sau:

1. Bật tính năng sao chép gói cập nhật đến một thư mục được chia sẻ trên một máy tính trên mạng máy tính cục bộ.
2. Thiết lập việc cập nhật của Kaspersky Endpoint Security từ thư mục được chia sẻ được quy định đến các máy tính còn lại trên mạng máy tính cục bộ.

Để bật việc sao chép gói cập nhật đến thư mục được chia sẻ:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Tác vụ được lập lịch**, chọn **Cập nhật**.
   Cấu hình Cập nhật Ứng dụng sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Trong phần **Bổ sung**, chọn hộp kiểm **Sao chép dữ liệu cập nhật tới thư mục**.
4. Nhập đường dẫn đến thư mục chia sẻ để đặt gói cập nhật. Bạn có thể làm việc này bằng một trong những cách sau đây:
   - Nhập đường dẫn đến thư mục được chia sẻ trong trường ở dưới hộp kiểm **Sao chép dữ liệu cập nhật tới thư mục**.
   - Nhấn nút **Duyệt**. Sau đó, trong cửa sổ **Lựa chọn thư mục** được mở ra, chọn thư mục cần thiết và nhấn **OK**.
5. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Để thiết lập việc cập nhật của Kaspersky Endpoint Security từ một thư mục được chia sẻ:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Tác vụ được lập lịch**, chọn **Cập nhật**.
   Cấu hình Cập nhật Ứng dụng sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Trong mục **Chế độ chạy và nguồn cập nhật**, nhấn nút **Nguồn cập nhật**.
   Việc này sẽ mở ra thẻ **Nguồn** trong cửa sổ **Cập nhật**.
4. Trên thẻ **Nguồn**, nhấn nút **Thêm**.
   Cửa sổ **Lựa chọn nguồn cập nhật** sẽ được mở ra.
5. Trong cửa sổ **Lựa chọn nguồn cập nhật**, chọn thư mục được chia sẻ có chứa gói cập nhật hoặc nhập đường dẫn đầy đủ đến thư mục được chia sẻ trong trường **Nguồn**.
6. Nhấn **OK**.

7. Trên thẻ **Nguồn**, xóa hộp kiểm cạnh tên của các nguồn cập nhật mà bạn không quy định là thư mục được chia sẻ.

8. Nhấn **OK**.

9. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Chọn chế độ chạy tác vụ cập nhật

Để chọn chế độ chạy tác vụ cập nhật:

1. Mở cửa sổ cấu hình ứng dụng.

2. Trong phần bên trái của cửa sổ, trong mục **Tác vụ được lập lịch**, chọn **Cập nhật**.
   Cấu hình Cập nhật Ứng dụng sẽ được hiển thị ở phần bên phải của cửa sổ.

3. Nhấn nút **Chế độ chạy**.
   Thẻ **Chế độ chạy** sẽ được mở ra trong cửa sổ **Cập nhật**.

4. Trong mục **Chế độ chạy**, chọn một trong nhiều tùy chọn để bắt đầu một tác vụ cập nhật:

   - Nếu bạn muốn Kaspersky Endpoint Security chạy tác vụ cập nhật tùy thuộc vào việc liệu có một gói cập nhật tại nguồn cập nhật hay không, hãy chọn **Tự động**. Tần suất kiểm tra gói cập nhật của Kaspersky Endpoint Security sẽ tăng lên trong các kỳ bùng phát virus và giảm vào các thời gian khác.

   - Nếu bạn muốn khởi động thủ công một tác vụ cập nhật, chọn **Thủ công**.

   - Nếu bạn muốn thiết lập một lịch khởi động tác vụ cập nhật, chọn **Theo lập lịch**.

5. Thực hiện một trong các thao tác sau:

   - Nếu bạn đã chọn **Tự động** hoặc **Thủ công**, đến bước 6 trong chỉ dẫn.

   - Nếu bạn đã chọn mục **Theo lập lịch**, hãy quy định cấu hình của lịch chạy tác vụ cập nhật. Để làm điều này:

     a. Trong danh sách thả xuống **Tần suất**, quy định khi nào thì chạy tác vụ cập nhật. Chọn một trong các tùy chọn sau: **Phút**, **Giờ**, **Ngày**, **Mỗi tuần**, **Vào một thời điểm được chỉ định**, **Mỗi tháng**, hoặc **Sau khi ứng dụng khởi động**.

     b. Tùy thuộc vào các mục được chọn từ danh sách thả xuống **Tần suất**, quy định giá trị cho cấu hình xác định thời gian khởi động tác vụ cập nhật.

     c. Trong trường **Tạm hoãn thực thi tác vụ sau khi khởi động ứng dụng trong**, quy định khoảng thời gian tạm hoãn việc khởi động tác vụ cập nhật sau khi Kaspersky Endpoint Security được khởi chạy.

     > Nếu đề mục **Sau khi ứng dụng khởi động** được chọn từ danh sách thả xuống **Tần suất**, trường **Tạm hoãn thực thi tác vụ sau khi khởi động ứng dụng trong** sẽ không thể được sử dụng.

d. Nếu bạn muốn Kaspersky Endpoint Security bắt đầu tác vụ cập nhật bị lỡ ngay khi có thể, chọn hộp kiểm **Chạy các tác vụ đã bị bỏ qua**.

> Nếu các đề mục **Giờ**, **Phút** hoặc **Sau khi ứng dụng khởi động** được chọn từ danh sách thả xuống **Tần suất**, hộp kiểm **Chạy các tác vụ đã bị bỏ qua** sẽ không thể được sử dụng.

6. Nhấn **OK**.

7. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Bắt đầu một tác vụ cập nhật theo quyền của một tài khoản người dùng khác

Theo mặc định, tác vụ cập nhật của Kaspersky Endpoint Security sẽ được bắt đầu theo tài khoản người dùng hiện tại mà bạn đã dùng để đăng nhập vào hệ điều hành. Tuy nhiên, Kaspersky Endpoint Security có thể được cập nhật từ một nguồn cập nhật mà người dùng không thể truy cập do thiếu quyền cần thiết (ví dụ, từ một thư mục được chia sẻ có chứa một gói cập nhật) hoặc không có quyền của một người dùng máy chủ proxy được phép. Trong cấu hình Kaspersky Endpoint Security, bạn có thể quy định một người dùng có các quyền đó và bắt đầu tác vụ cập nhật Kaspersky Endpoint Security theo tài khoản người dùng đó.

Để bắt đầu một tác vụ cập nhật theo một tài khoản người dùng khác:

1. Mở cửa sổ cấu hình ứng dụng.

2. Trong phần bên trái của cửa sổ, trong mục **Tác vụ được lập lịch**, chọn **Cập nhật**.
   Cấu hình Cập nhật Ứng dụng sẽ được hiển thị ở phần bên phải của cửa sổ.

3. Trong mục **Chế độ chạy và nguồn cập nhật**, nhấn nút **Chế độ chạy**.
   Thẻ **Chế độ chạy** sẽ được mở ra trong cửa sổ **Cập nhật**.

4. Trên thẻ **Chế độ chạy**, trong mục **Người dùng**, chọn hộp kiểm **Chạy tác vụ như**.

5. Trong trường **Tên**, nhập tên của tài khoản người dùng có quyền cần thiết để truy cập nguồn cập nhật.

6. Trong trường **Mật khẩu**, nhập mật khẩu của người dùng có quyền cần thiết để truy cập nguồn cập nhật.

7. Nhấn **OK**.

8. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Thiết lập việc cập nhật các mô-đun ứng dụng

Để thiết lập việc cập nhật các mô-đun ứng dụng:

1. Mở cửa sổ cấu hình ứng dụng.

2. Trong phần bên trái của cửa sổ, trong mục **Tác vụ được lập lịch**, chọn **Cập nhật**.

   Cấu hình Cập nhật Ứng dụng sẽ được hiển thị ở phần bên phải của cửa sổ.

3. Trong mục **Bổ sung**, thực hiện một trong những hành động sau:

   - Chọn hộp kiểm **Tải bản cập nhật của mô-đun ứng dụng** nếu bạn muốn ứng dụng bao gồm các bản cập nhật mô-đun ứng dụng trong gói cập nhật.
   - Nếu không, xóa hộp kiểm **Tải bản cập nhật của mô-đun ứng dụng**.

4. Nếu hộp kiểm **Tải bản cập nhật của mô-đun ứng dụng** được chọn ở bước trước, quy định các điều kiện mà theo đó ứng dụng sẽ cài đặt bản cập nhật mô-đun ứng dụng:

   - Chọn **Cài đặt bản cập nhật quan trọng và đã được phê duyệt** nếu bạn muốn ứng dụng tự động cài đặt các bản cập nhật thiết yếu của mô-đun ứng dụng, và các bản cập nhật khác sau khi việc cài đặt chúng được phê duyệt cục bộ thông qua giao diện ứng dụng hoặc sử dụng Kaspersky Security Center.
   - Chọn **Chỉ cài đặt bản cập nhật đã được phê duyệt** nếu bạn muốn ứng dụng chỉ cài đặt các bản cập nhật mô-đun ứng dụng sau khi việc cài đặt chúng đã được phê duyệt cục bộ thông qua giao diện ứng dụng hoặc sử dụng Kaspersky Security Center.

5. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Bắt đầu và dừng một tác vụ cập nhật

Bất kể chế độ chạy tác vụ cập nhật được chọn, bạn đều có thể bắt đầu hoặc dừng một tác vụ cập nhật Kaspersky Endpoint Security bất cứ lúc nào.

Để tải một gói cập nhật từ máy chủ của Kaspersky, bạn cần có một kết nối Internet.

Để bắt đầu hoặc dừng một tác vụ cập nhật:

1. Mở cửa sổ chính của ứng dụng.
2. Chọn thẻ **Bảo vệ và Kiểm soát**.
3. Nhấn vào mục **Tác vụ**.

   Mục **Tác vụ** sẽ được mở ra.

4. Nhấn phải chuột để gọi menu ngữ cảnh của dòng có chứa tên tác vụ cập nhật.

   Nhấn vào dòng này để mở ra một menu hành động được thực hiện trên tác vụ cập nhật.

5. Thực hiện một trong các thao tác sau:

   - Nếu bạn muốn bắt đầu tác vụ cập nhật, chọn **Bắt đầu cập nhật** từ menu.

     Trạng thái tiến độ của tác vụ cập nhật được hiển thị ở bên phải của nút **Cập nhật** sẽ được chuyển thành *Đang chạy*.

   - Nếu bạn muốn dừng tác vụ cập nhật, chọn **Dừng cập nhật** từ menu.

Trạng thái tiến độ của tác vụ cập nhật được hiển thị ở bên phải của nút **Cập nhật** sẽ được chuyển thành *Đã dừng*.

Khôi phục lại bản cập nhật gần nhất

Sau khi cơ sở dữ liệu và các mô-đun ứng dụng được cập nhật lần đầu tiên, chức năng khôi phục lại cơ sở dữ liệu và các mô-đun ứng dụng về phiên bản trước đó sẽ có thể được sử dụng.

Mỗi khi người dùng bắt đầu tiến trình cập nhật, Kaspersky Endpoint Security sẽ tạo một bản sao dự phòng của các cơ sở dữ liệu và mô-đun ứng dụng hiện tại. Điều này cho phép bạn khôi phục lại cơ sở dữ liệu và các mô-đun ứng dụng về phiên bản trước đó khi cần thiết. Tính năng khôi phục lại bản cập nhật trước là rất hữu ích, chẳng hạn như khi phiên bản cơ sở dữ liệu mới chứa một chữ ký không hợp lệ khiến Kaspersky Endpoint Security chặn một ứng dụng an toàn.

Để khôi phục lại bản cập nhật gần nhất:

1. Mở cửa sổ chính của ứng dụng.
2. Chọn thẻ **Bảo vệ và Kiểm soát**.
3. Nhấn vào mục **Tác vụ**.
   Mục **Tác vụ** sẽ được mở ra.
4. Nhấn phải chuột để gọi menu ngữ cảnh của tác vụ **Cập nhật**.
5. Chọn **khôi phục lại cập nhật**.

Thiết lập cấu hình máy chủ proxy

Để thiết lập cấu hình máy chủ proxy:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Tác vụ được lập lịch**, chọn **Cập nhật**.
   Cấu hình Cập nhật Ứng dụng sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Trong mục **Máy chủ proxy**, nhấn nút **Cấu hình**.
   Cửa sổ **Cấu hình máy chủ proxy** sẽ được mở ra.
4. Trong cửa sổ **Cấu hình máy chủ proxy**, chọn hộp kiểm **Sử dụng máy chủ proxy**.
5. Quy định cấu hình máy chủ proxy.
6. Nhấn **OK**.
7. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Bạn cũng có thể thiết lập cấu hình máy chủ proxy trong cửa sổ chính của ứng dụng, trên thẻ **Cấu hình**, trong mục **Cấu hình nâng cao**.

Quét máy tính

Một tác vụ quét virus là thiết yếu cho bảo mật máy tính. Các tác vụ quét virus được chạy thường xuyên giúp loại trừ nguy cơ phân tán phần mềm độc hại không được phát hiện bởi các thành phần bảo vệ do cấu hình bảo mật thấp hoặc vì các lý do khác.

Mục này mô tả chi tiết và cấu hình của các tác vụ quét, cấp độ bảo mật, phương thức và công nghệ quét, và hướng dẫn cách xử lý các tập tin chưa được Kaspersky Endpoint Security xử lý trong một tác vụ quét virus.

Thông tin về tác vụ quét

Để tìm virus và các loại phần mềm độc hại khác, cũng như kiểm tra tính toàn vẹn của các mô-đun ứng dụng, Kaspersky Endpoint Security sẽ bao gồm các tác vụ sau:

- **Quét Toàn bộ**. Quét kỹ lưỡng toàn bộ máy tính. Theo mặc định, Kaspersky Endpoint Security sẽ quét các đối tượng sau:
  - Bộ nhớ kernel
  - Các đối tượng được nạp lúc khởi động hệ điều hành
  - Phân vùng khởi động
  - Bản sao hệ điều hành
  - Toàn bộ ổ cứng và ổ đĩa di động
- **Quét khu vực quan trọng**. Theo mặc định, Kaspersky Endpoint Security sẽ quét nhân kernel, các tiến trình đang chạy, và phân vùng khởi động ổ đĩa.
- **Quét Tùy chỉnh**. Kaspersky Endpoint Security sẽ quét các đối tượng được chọn bởi người dùng. Bạn có thể quét bất kỳ đối tượng nào từ danh sách sau đây:
  - Bộ nhớ kernel
  - Các đối tượng được nạp lúc khởi động hệ điều hành
  - Bản sao hệ điều hành
  - Hộp thư Outlook
  - Tất cả các ổ cứng, ổ đĩa di động và ổ đĩa mạng
  - Bất kỳ tập tin nào được lựa chọn
- **Kiểm tra Tính Toàn vẹn**. Kaspersky Endpoint Security sẽ kiểm tra các mô-đun ứng dụng để phát hiện hư hỏng hoặc sửa đổi.

Các tác vụ Quét Toàn bộ và Quét khu vực quan trọng hơi khác so với các tác vụ khác. Đối với các tác vụ này, bạn không nên sửa phạm vi quét.

Sau khi tác vụ quét được bắt đầu, tiến trình hoàn tất của chúng sẽ được hiển thị trong trường cạnh tên của tác vụ quét đang chạy, trong mục **Tác vụ** trên thẻ **Bảo vệ và Kiểm soát** của cửa sổ chính của Kaspersky Endpoint Security.

Thông tin về kết quả quét và các sự kiện đã xảy ra trong quá trình thực thi tác vụ quét được ghi lại trong một báo cáo của Kaspersky Endpoint Security.

Bắt đầu hoặc dừng một tác vụ quét

Bất kể chế độ chạy tác vụ quét được chọn, bạn đều có thể bắt đầu hoặc dừng một tác vụ quét bất cứ lúc nào.

Để bắt đầu hoặc dừng một tác vụ quét:

1. Mở cửa sổ chính của ứng dụng.
2. Chọn thẻ **Bảo vệ và Kiểm soát**.
3. Nhấn vào mục **Tác vụ**.

   Mục **Tác vụ** sẽ được mở ra.
4. Nhấn phải chuột để gọi menu ngữ cảnh của dòng có chứa tên tác vụ quét.

   Một menu với hành động tác vụ quét sẽ được mở ra.
5. Thực hiện một trong các thao tác sau:

   - Nếu bạn muốn bắt đầu tác vụ quét, chọn **Bắt đầu quét** từ menu.

     Trạng thái tiến độ tác vụ được hiển thị ở bên phải của nút với tên của tác vụ quét này sẽ được chuyển thành *Đang chạy*.
   - Nếu bạn muốn dừng tác vụ quét, chọn **Dừng quét** từ menu.

     Trạng thái tiến độ tác vụ được hiển thị ở bên phải của nút với tên của tác vụ quét này sẽ được chuyển thành *Đã dừng*.

Thiết lập cấu hình của tác vụ quét

Để thiết lập cấu hình của tác vụ quét, bạn có thể thực hiện các hành động sau:

- Thay đổi cấp độ bảo mật.

  Bạn có thể chọn một trong các cấp độ bảo mật được thiết lập sẵn hoặc tự cấu hình thiết lập cấp độ bảo mật. Nếu bạn đã thay đổi thiết lập cấp độ bảo mật, bạn luôn có thể quay lại thiết lập cấp độ bảo mật được khuyến nghị.
- Thay đổi hành động được Kaspersky Endpoint Security thực hiện nếu ứng dụng phát hiện một tập tin bị nhiễm.
- Sửa phạm vi quét.

  Bạn có thể mở rộng hoặc hạn chế phạm vi quét bằng cách thêm hoặc xóa các đối tượng quét, hoặc bằng cách thay đổi loại tập tin được quét.

- Tối ưu quét.

  Bạn có thể tối ưu tác vụ quét tập tin: giảm thiểu thời gian quét và tăng tốc độ hoạt động của Kaspersky Endpoint Security. Điều này có thể có được bằng cách chỉ quét các tập tin mới và các tập tin đã được thay đổi kể từ lần quét gần nhất. Chế độ này được áp dụng cho cả các tập tin đơn và tập tin hỗn hợp. Bạn cũng có thể đặt giới hạn để quét một tập tin. Khi khoảng thời gian được quy định đã trôi qua, Kaspersky Endpoint Security sẽ loại trừ tập tin này khỏi tác vụ quét hiện tại (ngoại trừ các tập nén và đối tượng bao gồm nhiều tập tin).

  Bạn cũng có thể bật các công nghệ iChecker và iSwift. Những công nghệ này giúp tối ưu tốc độ quét tập tin bằng cách loại trừ các tập tin chưa được thay đổi kể từ lần quét gần nhất.

- Thiết lập quét các tập tin hỗn hợp.

- Thiết lập việc sử dụng các phương thức quét.

  Khi kích hoạt, Kaspersky Endpoint Security sẽ sử dụng phân tích dấu hiệu. Trong quá trình phân tích dấu hiệu, Kaspersky Endpoint Security sẽ đối chiếu đối tượng được phát hiện với các hồ sơ trong cơ sở dữ liệu của ứng dụng. Theo khuyến nghị của các chuyên gia Kaspersky, tính năng phân tích dấu hiệu luôn được bật.

  Để tăng hiệu quả bảo vệ, bạn có thể sử dụng phân tích suy nghiệm. Trong phân tích suy nghiệm, Kaspersky Endpoint Security sẽ phân tích hoạt động của các đối tượng trong hệ điều hành. Phân tích suy nghiệm có thể phát hiện các đối tượng độc hại không có hồ sơ trong cơ sở dữ liệu của Kaspersky Endpoint Security.

- Chọn chế độ chạy cho tác vụ quét.

  Nếu không thể chạy tác vụ quét vì bất cứ lý do gì (ví dụ, máy tính đang tắt tại thời điểm đó), bạn có thể thiết lập tác vụ bị bỏ qua được tự động bắt đầu ngay khi có thể.

  Bạn có thể hoãn việc bắt đầu tác vụ quét sau khi ứng dụng khởi động nếu chọn chế độ chạy tác vụ quét **Theo lập lịch**, và nếu thời gian khởi động của Kaspersky Endpoint Security khớp với lịch khởi động tác vụ quét. Tác vụ quét chỉ có thể được chạy sau khoảng thời gian được quy định từ lúc khởi động Kaspersky Endpoint Security.

- Thiết lập tác vụ quét để chạy theo một tài khoản người dùng khác.

- Quy định cấu hình quét ổ đĩa di động khi chúng được kết nối.

Thay đổi cấp độ bảo mật

Để thực hiện tác vụ quét, Kaspersky Endpoint Security sẽ sử dụng nhiều cấu hình khác nhau. Các nhóm thiết lập được lưu trong ứng dụng này được gọi là *cấp độ bảo mật*. Có 3 cấp độ bảo mật được thiết lập sẵn: **Cao**, **Khuyên dùng**, và **Thấp**. Thiết lập cấp độ bảo mật **Khuyến khích** được coi là tối ưu. Chúng được khuyến nghị bởi các chuyên gia Kaspersky.

Để thay đổi một cấp độ bảo mật:

1. Mở cửa sổ cấu hình ứng dụng.

2. Trong phần bên trái của cửa sổ, trong mục **Tác vụ được lập lịch**, chọn mục con chứa tên của tác vụ quét cần thiết (**Quét Toàn bộ**, **Quét khu vực quan trọng** hoặc **Quét Tùy chỉnh**).

   Ở phần bên phải của cửa sổ, cấu hình của tác vụ quét được chọn sẽ được hiển thị.

3. Trong mục **Mức độ bảo mật**, thực hiện một trong những hành động sau:

- Nếu bạn muốn áp dụng một trong những cấp độ bảo mật được thiết lập sẵn (**Cao**, **Khuyên dùng**, hoặc **Thấp**), hãy chọn nó với thanh trượt.
- Nếu bạn muốn cấu hình một cấp độ bảo mật tùy chỉnh, chọn nút **Thiết lập** và trong cửa sổ được mở ra, nhập thiết lập với tên của tác vụ quét.

  Sau khi bạn thiết lập một cấp độ bảo mật tùy chỉnh, tên của cấp độ bảo mật trong mục **Mức độ bảo mật** sẽ được chuyển thành **Tùy chỉnh**.
- Nếu bạn muốn thay đổi cấp độ bảo mật thành **Khuyên dùng**, nhấn nút **Mặc định**.

4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Thay đổi hành động xử lý tập tin bị nhiễm

Để thay đổi hành động xử lý tập tin bị nhiễm:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Tác vụ được lập lịch**, chọn mục con chứa tên của tác vụ quét cần thiết (**Quét Toàn bộ**, **Quét khu vực quan trọng** hoặc **Quét Tùy chỉnh**).

   Ở phần bên phải của cửa sổ, cấu hình của tác vụ quét được chọn sẽ được hiển thị.
3. Trong mục **Hành động khi phát hiện nguy hiểm**, chọn các tùy chọn cần thiết:
   - **Lựa chọn hành động tự động**.
   - **Đề xuất xử lý**.
4. Nếu bạn đã chọn mục **Đề xuất xử lý** ở bước trước, hãy chọn các hộp kiểm sau đây:
   - Chọn hộp kiểm **Khử mã độc** nếu bạn muốn Kaspersky Endpoint Security khử nhiễm các đối tượng được phát hiện là có chứa mối đe dọa.

     Nếu mục này được chọn, Kaspersky Endpoint Security sẽ áp dụng hành động **Gỡ bỏ** đến các tập tin là một phần của ứng dụng Windows Store.
   - Chọn hộp kiểm **Xóa** nếu bạn muốn Kaspersky Endpoint Security xóa các đối tượng được phát hiện là có chứa mối đe dọa.
   - Chọn cả hai hộp kiểm **Khử nhiễm** và **Khử mã độc** nếu bạn muốn Kaspersky Endpoint Security cố gắng khử nhiễm các đối tượng được phát hiện là có chứa mối đe dọa, và xóa các đối tượng không thể được khử nhiễm.
   - Xóa cả hai hộp kiểm **Khử nhiễm** và **Khử mã độc** nếu bạn muốn Kaspersky Endpoint Security không thực hiện bất cứ hành động nào đối với các đối tượng được phát hiện là có chứa mối đe dọa, thay vào đó chỉ thông báo với người dùng về kết quả quét các đối tượng này.
5. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Đang tạo một danh sách các đối tượng cần quét

Để tạo một danh sách các đối tượng cần quét, bạn có thể sử dụng một trong hai phương thức sau đây:

- Trên thẻ **Bảo vệ và Kiểm soát** của cửa sổ chính của ứng dụng
- Từ cửa sổ cấu hình ứng dụng.

> Phương thức này chỉ khả dụng cho các tác vụ **Quét toàn bộ** và **Quét khu vực quan trọng**. Danh sách các đối tượng cần quét cho tác vụ **Quét tùy chỉnh** chỉ có thể được tạo trên thẻ **Bảo vệ và kiểm soát**.

Để tạo một danh sách các đối tượng cần quét trên thẻ Bảo vệ và Kiểm soát của cửa sổ chính của ứng dụng:

1. Mở cửa sổ chính của ứng dụng.
2. Chọn thẻ **Bảo vệ và Kiểm soát**.
3. Nhấn vào mục **Tác vụ**.
   Mục **Tác vụ** sẽ được mở ra.
4. Nhấn chuột phải để mở menu ngữ cảnh của dòng chứa tên tác vụ và chọn **Phạm vi quét**.
   Cửa sổ **Phạm vi quét** sẽ được mở ra.
5. Nếu bạn muốn bổ sung một đối tượng mới vào phạm vi quét:
   a. Nhấn vào nút **Thêm**.
      Cửa sổ **Lựa chọn phạm vi quét** sẽ được mở ra.
   b. Chọn đối tượng và nhấn **Thêm**.
      Tất cả các đối tượng được chọn trong cửa sổ **Lựa chọn phạm vi quét** đều được hiển thị trong danh sách **Phạm vi quét**.
   c. Nhấn **OK**.
6. Nếu bạn muốn thay đổi đường dẫn đến một đối tượng trong phạm vi quét:
   a. Chọn đối tượng trong phạm vi quét.
   b. Nhấn nút **Chỉnh sửa**.
      Cửa sổ **Lựa chọn phạm vi quét** sẽ được mở ra.
   c. Nhập đường dẫn mới đến đối tượng trong phạm vi quét.
   d. Nhấn **OK**.
7. Nếu bạn muốn xóa một đối tượng khỏi phạm vi quét:
   a. Chọn đối tượng mà bạn muốn xóa khỏi phạm vi quét.

Để chọn nhiều đối tượng, giữ nút **CTRL** khi chọn chúng.

b. Nhấn nút **Gỡ bỏ**.

Một cửa sổ để xác nhận việc xóa sẽ được mở ra.

c. Nhấn nút **Có** trong cửa sổ xác nhận xóa.

> Bạn không thể xóa hoặc sửa các đối tượng được bao gồm trong phạm vi quét mặc định.

8. Để loại trừ một đối tượng khỏi phạm vi quét, xóa hộp kiểm cạnh đối tượng đó trong cửa sổ **Phạm vi quét**.

   Đối tượng vẫn sẽ có tên trong danh sách các đối tượng trong phạm vi quét, nhưng nó sẽ không bị quét khi tác vụ quét được chạy.

9. Nhấn **OK**.

10. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Để tạo một danh sách các đối tượng cần quét từ cửa sổ thiết lập ứng dụng:

1. Mở cửa sổ cấu hình ứng dụng.

2. Trong phần bên trái của cửa sổ, trong mục **Tác vụ được lập lịch**, chọn mục con với tên của tác vụ quét cần thiết: **Quét toàn bộ**, hoặc **Quét khu vực quan trọng**.

   Ở phần bên phải của cửa sổ, cấu hình của tác vụ quét được chọn sẽ được hiển thị.

3. Nhấn nút **Phạm vi quét**.

   Cửa sổ **Phạm vi quét** sẽ được mở ra.

4. Tạo một danh sách các đối tượng cần quét theo các bước 5-10 của chỉ dẫn trước.

Chọn loại tập tin cần quét

Bạn có thể sử dụng hai phương thức để chọn loại tập tin cần quét:

- Trên thẻ **Bảo vệ và Kiểm soát** của cửa sổ chính của ứng dụng
- Từ cửa sổ cấu hình ứng dụng.

> Phương thức này chỉ khả dụng cho các tác vụ **Quét toàn bộ** và **Quét khu vực quan trọng**. Các loại tập tin cần quét cho tác vụ **Quét tùy chỉnh** chỉ có thể được chọn trên thẻ **Bảo vệ và kiểm soát**.

Để chọn loại tập tin cần quét trên thẻ Bảo vệ và kiểm soát của cửa sổ chính của ứng dụng:

1. Mở cửa sổ chính của ứng dụng.

2. Chọn thẻ **Bảo vệ và Kiểm soát**.

3. Nhấn vào mục **Tác vụ**.

   Mục **Tác vụ** sẽ được mở ra.

4. Nhấn chuột phải để mở menu ngữ cảnh của dòng chứa tên tác vụ và chọn **Thiết lập**.

   Một cửa sổ với tên của tác vụ quét được chọn sẽ được mở ra.

5. Trong cửa sổ với tên của tác vụ quét được chọn, chọn thẻ **Phạm vi**.

6. Trong mục **Loại tập tin**, quy định loại tập tin mà bạn muốn quét khi chạy tác vụ quét được chọn:

   - Nếu bạn muốn quét tất cả các tập tin, chọn **Tất cả các tập tin**.
   - Nếu bạn muốn quét các tập tin có định dạng dễ bị nhiễm virus nhất, hãy chọn **Quét các tập tin theo phần định dạng**.
   - Nếu bạn muốn quét các tập tin có phần mở rộng dễ bị nhiễm virus nhất, hãy chọn **Quét các tập tin theo phần mở rộng**.

   Khi chọn loại tập tin để quét, hãy cân nhắc các thông tin sau:

   - Có một số định dạng tập tin (ví dụ như TXT) mà khả năng xâm nhập và kích hoạt mã độc trên đó là rất thấp. Mặt khác, cũng có những tập tin chứa hoặc có thể chứa các mã thực thi (ví dụ như .exe, .dll và .doc). Nguy cơ xâm nhập và kích hoạt mã độc trên các tập tin này là cao.
   - Một kẻ xâm nhập có thể gửi một virus hoặc một chương trình độc hại khác đến máy tính của bạn trong một tập tin thực thi đã được đổi tên để chứa phần mở rộng .txt. Nếu bạn chọn quét tập tin theo phần mở rộng, ứng dụng sẽ bỏ qua tập tin này trong quá trình quét. Nếu chọn quét tập tin theo định dạng, Chống virus cho tập tin sẽ phân tích đầu mục tập tin bất kể phần mở rộng là gì. Nếu phân tích này cho thấy tập tin có định dạng EXE, ứng dụng sẽ quét nó.

7. Trong cửa sổ chứa tên của tác vụ quét, nhấn nút **OK**.

8. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Để chọn loại tập tin cần quét từ cửa sổ thiết lập ứng dụng:

1. Mở cửa sổ cấu hình ứng dụng.

2. Trong phần bên trái của cửa sổ, trong mục **Tác vụ được lập lịch**, chọn mục con với tên của tác vụ quét cần thiết: **Quét toàn bộ**, hoặc **Quét khu vực quan trọng**.

   Ở phần bên phải của cửa sổ, cấu hình của tác vụ quét được chọn sẽ được hiển thị.

3. Trong mục **Mức độ bảo mật**, nhấn nút **Cấu hình**.

   Một cửa sổ với tên của tác vụ quét được chọn sẽ được mở ra.

4. Trong cửa sổ với tên của tác vụ quét được chọn, chọn thẻ **Phạm vi**.

5. Hoàn thành các bước 5-7 của hướng dẫn trước.

Tối ưu quét tập tin

Để tối ưu quét tập tin:

1. Mở cửa sổ cấu hình ứng dụng.

2. Trong phần bên trái của cửa sổ, trong mục **Tác vụ được lập lịch**, chọn mục con chứa tên của tác vụ quét cần thiết (**Quét Toàn bộ**, **Quét khu vực quan trọng** hoặc **Quét Tùy chỉnh**).

   Ở phần bên phải của cửa sổ, cấu hình của tác vụ quét được chọn sẽ được hiển thị.

3. Trong mục **Mức độ bảo mật**, nhấn nút **Cấu hình**.

   Một cửa sổ với tên của tác vụ quét được chọn sẽ được mở ra.

4. Trong cửa sổ được mở ra, chọn thẻ **Phạm vi**.

5. Trong mục **Tối ưu quét**, thực hiện các hành động sau:

   - Chọn hộp kiểm **Chỉ quét các tập tin mới hoặc có sự thay đổi**.
   - Chọn hộp kiểm **Bỏ qua các tập tin quét trong thời gian dài** và quy định thời gian quét cho một tập tin duy nhất (tính theo giây).

6. Nhấn **OK**.

7. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Quét các tập tin hỗn hợp

Một kỹ thuật phổ biến để che giấu virus và các phần mềm độc hại khác là nhúng chúng trong các tập tin tổ hợp ví dụ như tập nén hoặc cơ sở dữ liệu. Để phát hiện virus và các phần mềm độc hại khác được ẩn giấu bằng cách này, tập tin hỗn hợp phải được giải nén, điều này có thể làm giảm tốc độ quét. Bạn có thể giới hạn loại tập tin hỗn hợp được quét để tăng tốc độ quét.

Để thiết lập quét các tập tin hỗn hợp:

1. Mở cửa sổ cấu hình ứng dụng.

2. Trong phần bên trái của cửa sổ, trong mục **Tác vụ được lập lịch**, chọn mục con chứa tên của tác vụ quét cần thiết (**Quét Toàn bộ**, **Quét khu vực quan trọng** hoặc **Quét Tùy chỉnh**).

   Ở phần bên phải của cửa sổ, cấu hình của tác vụ quét được chọn sẽ được hiển thị.

3. Trong mục **Mức độ bảo mật**, nhấn nút **Cấu hình**.

   Một cửa sổ với tên của tác vụ quét được chọn sẽ được mở ra.

4. Trong cửa sổ được mở ra, chọn thẻ **Phạm vi**.

5. Trong mục **Quét các tập tin hỗn hợp**, quy định các tập tin hỗn hợp mà bạn muốn quét: tập nén, gói cài đặt, tập tin trong định dạng office, tập tin trong định dạng email, và các tập nén có mật khẩu bảo vệ.

6. Nếu hộp kiểm **Chỉ quét các tập tin mới hoặc có sự thay đổi** bị xóa trong mục **Tối ưu quét**, nhấn vào liên kết **tất cả / mới** cạnh tên của loại tập tin hỗn hợp nếu bạn muốn quy định cho từng loại tập tin hỗn hợp để quét tất cả các tập tin thuộc thể loại này, hay chỉ quét các tập tin mới thuộc thể loại này.

   Liên kết này sẽ thay đổi giá trị khi nó được nhấn.

Nếu hộp kiểm **Chỉ quét các tập tin mới hoặc có sự thay đổi** được chọn, chỉ các tập tin mới mới được quét.

7. Nhấn nút **Bổ sung**.

   Cửa sổ **Các tập tin hỗn hợp** sẽ được mở ra.

8. Trong mục **Dung lượng giới hạn**, thực hiện một trong những hành động sau:

   - Nếu bạn không muốn giải nén các tập tin hỗn hợp quá lớn, chọn hộp kiểm **Không thực hiện giải nén các tập tin hỗn hợp lớn** và quy định giá trị cần thiết trong trường **Dung lượng tối đa của tập tin**.
   - Nếu bạn muốn giải nén các tập tin hỗn hợp lớn bất kể kích cỡ của chúng là gì, xóa hộp kiểm **Không thực hiện giải nén các tập tin hỗn hợp lớn**.

   Kaspersky Endpoint Security sẽ quét các tập tin lớn được giải nén từ tập nén, bất kể là hộp kiểm **Không thực hiện giải nén các tập tin hỗn hợp lớn** có được chọn hay không.

9. Nhấn **OK**.

10. Trong cửa sổ chứa tên của tác vụ quét, nhấn nút **OK**.

11. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Sử dụng các phương thức quét

Để sử dụng các phương thức quét:

1. Mở cửa sổ cấu hình ứng dụng.

2. Trong phần bên trái của cửa sổ, trong mục **Tác vụ được lập lịch**, chọn mục con chứa tên của tác vụ quét cần thiết (**Quét Toàn bộ**, **Quét khu vực quan trọng** hoặc **Quét Tùy chỉnh**).

   Ở phần bên phải của cửa sổ, cấu hình của tác vụ quét được chọn sẽ được hiển thị.

3. Trong mục **Mức độ bảo mật**, nhấn nút **Cấu hình**.

   Một cửa sổ với tên của tác vụ quét được chọn sẽ được mở ra.

4. Trong cửa sổ được mở ra, chọn thẻ **Bổ sung**.

5. Nếu bạn muốn ứng dụng sử dụng phân tích suy nghiệm khi chạy tác vụ quét, trong mục **Phương thức quét**, chọn hộp kiểm Phân tích suy nghiệm. Sau đó sử dụng thanh trượt để đặt cấp độ phân tích suy nghiệm: **Quét nhanh**, **quét vừa**, hoặc **quét kỹ**.

6. Nhấn **OK**.

7. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Sử dụng các công nghệ quét

Để sử dụng các công nghệ quét:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Tác vụ được lập lịch**, chọn mục con chứa tên của tác vụ quét cần thiết (**Quét Toàn bộ**, **Quét khu vực quan trọng** hoặc **Quét Tùy chỉnh**).

   Ở phần bên phải của cửa sổ, cấu hình của tác vụ quét được chọn sẽ được hiển thị.
3. Trong mục **Mức độ bảo mật**, nhấn nút **Cấu hình**.

   Một cửa sổ với tên của tác vụ quét được chọn sẽ được mở ra.
4. Trong cửa sổ được mở ra, chọn thẻ **Bổ sung**.
5. Trong mục **Các công nghệ quét**, chọn hộp kiểm cạnh tên của các công nghệ mà bạn muốn sử dụng trong tác vụ quét.
6. Nhấn **OK**.
7. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Chọn chế độ chạy cho tác vụ quét

Để chọn chế độ chạy cho tác vụ quét:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Tác vụ được lập lịch**, chọn mục con chứa tên của tác vụ cần thiết (**Quét Toàn bộ**, **Quét khu vực quan trọng** hoặc **Quét Tùy chỉnh**).

   Ở phần bên phải của cửa sổ, cấu hình của tác vụ quét được chọn sẽ được hiển thị.
3. Nhấn nút **Chế độ chạy**.

   Một cửa sổ với thuộc tính của tác vụ được chọn sẽ được mở ra trên thẻ **Chế độ chạy**.
4. Trong mục **Chế độ chạy**, chọn chế độ chạy tác vụ: **Thủ công** hoặc **Theo lập lịch**.
5. Nếu bạn đã chọn mục **Theo lập lịch**, hãy quy định cấu hình lịch. Để làm điều này:
   a. Trong danh sách thả xuống **Tần suất**, chọn tần suất chạy tác vụ (**Phút**, **Giờ**, **Ngày**, **Mỗi tuần**, **Vào một thời điểm được chỉ định**, **Mỗi tháng**, hoặc **Sau khi ứng dụng khởi động**, **Sau mỗi lần cập nhật**).
   b. Tùy thuộc vào tần suất được chọn, thiết lập cấu hình nâng cao quy định lịch chạy tác vụ.
   c. Nếu bạn muốn Kaspersky Endpoint Security bắt đầu tác vụ quét bị lỡ ngay khi có thể, chọn hộp kiểm **Chạy các tác vụ đã bị bỏ qua**.

   > Nếu các đề mục **Phút**, **Giờ**, **Sau khi ứng dụng khởi động** hoặc **Sau mỗi lần cập nhật** được chọn từ danh sách thả xuống **Tần suất**, hộp kiểm **Chạy các tác vụ đã bị bỏ qua** sẽ không thể được sử dụng.

a. Nếu bạn muốn Kaspersky Endpoint Security tạm ngưng một tác vụ khi tài nguyên máy tính bị hạn chế, chọn hộp kiểm **Chỉ chạy khi máy tính đang rảnh**.

   Tùy chọn lịch này giúp tiết kiệm tài nguyên máy tính.

6. Nhấn **OK**.

7. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Bắt đầu một tác vụ quét bằng tài khoản của một người dùng khác

Theo mặc định, một tác vụ quét được chạy với sự cho phép của tài khoản mà người dùng sử dụng để đăng nhập vào hệ điều hành. Tuy nhiên, bạn có thể cần chạy một tác vụ quét với một tài khoản người dùng khác. Bạn có thể quy định một người dùng có quyền phù hợp trong cấu hình của tác vụ quét và chạy tác vụ quét bằng tài khoản của người dùng này.

Để thiết lập việc bắt đầu một tác vụ quét bằng tài khoản của một người dùng khác:

1. Mở cửa sổ cấu hình ứng dụng.

2. Trong phần bên trái của cửa sổ, trong mục **Tác vụ được lập lịch**, chọn mục con chứa tên của tác vụ cần thiết (**Quét Toàn bộ**, **Quét khu vực quan trọng** hoặc **Quét Tùy chỉnh**).

   Ở phần bên phải của cửa sổ, cấu hình của tác vụ quét được chọn sẽ được hiển thị.

3. Nhấn nút **Chế độ chạy**.

   Việc này sẽ mở ra một cửa sổ với thuộc tính của tác vụ được chọn trên thẻ **Chế độ chạy**.

4. Trên thẻ **Chế độ chạy**, trong mục **Người dùng**, chọn hộp kiểm **Chạy tác vụ như**.

5. Trong trường **Tên**, nhập tên của tài khoản người dùng có quyền cần thiết để chạy tác vụ quét.

6. Trong trường **Mật khẩu**, nhập mật khẩu của người dùng có quyền cần thiết để chạy tác vụ quét.

7. Nhấn **OK**.

8. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Quét ổ đĩa di động khi chúng được kết nối với máy tính

Một số chương trình độc hại sẽ khai thác lỗ hổng bảo mật của hệ điều hành để lây lan qua các mạng cục bộ và ổ đĩa di động. Kaspersky Endpoint Security cho phép bạn quét các ổ đĩa di động được kết nối đến máy tính để phát hiện virus và các phần mềm độc hại khác.

Để thiết lập quét các ổ đĩa di động khi chúng được kết nối:

1. Mở cửa sổ cấu hình ứng dụng.

2. Ở phần bên trái của cửa sổ, chọn mục **Tác vụ được lập lịch**.

   Thiết lập của tác vụ sẽ được hiển thị ở phần bên phải của cửa sổ.

3. Trong mục **Quét các ổ cứng di động khi kết nối**, trong danh sách thả xuống **Hoạt động trên các thiết bị di động kết nối**, chọn hành động cần thiết:

   - **Không quét**
   - **Quét chi tiết**

     Trong chế độ này, Kaspersky Endpoint Security sẽ quét tất cả các tập tin có trên ổ đĩa di động, bao gồm các tập tin trong các đối tượng hỗn hợp.

   - **Quét nhanh**

     Trong chế độ này, Kaspersky Endpoint Security sẽ chỉ quét các tập tin có khả năng bị nhiễm, và không giải nén các đối tượng phức hợp.

4. Nếu bạn muốn Kaspersky Endpoint Security chỉ quét các ổ đĩa di động có kích cỡ không vượt quá một giá trị cụ thể, chọn hộp kiểm **Kích thước tối đa của ổ cứng di động** và quy định một giá trị theo megabyte trong trường cạnh nó.

5. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Xử lý các tập tin chưa được xử lý

Mục này chứa chỉ dẫn về cách để xử lý các tập tin bị nhiễm và có khả năng bị nhiễm nhưng chưa được Kaspersky Endpoint Security xử lý trong khi quét máy tính để phát hiện virus và các mối đe dọa khác.

Thông tin về các tập tin chưa được xử lý

Kaspersky Endpoint Security sẽ ghi lại thông tin về các tập tin mà nó chưa xử lý vì một lý do nào đó. Thông tin này được ghi lại dưới dạng các sự kiện trong danh sách các tập tin chưa được xử lý.

Một tập tin bị nhiễm được coi là *đã được xử lý* nếu Kaspersky Endpoint Security thực hiện một trong các hành động sau trên tập tin đó theo cấu hình được quy định của ứng dụng trong khi quét máy tính để phát hiện virus và các mối đe dọa khác:

- Khử nhiễm.
- Xóa.
- Xóa nếu khử nhiễm thất bại.

Một tập tin bị nhiễm được coi là *không được xử lý* nếu Kaspersky Endpoint Security vì bất cứ lý do gì đã không thực hiện một hành động trên tập tin đó theo cấu hình được quy định của ứng dụng trong khi quét máy tính để phát hiện virus và các mối đe dọa khác.

Tình huống này có thể xảy ra trong các trường hợp sau:

- Tập tin được quét không thể được truy cập (ví dụ, nó nằm trên một ổ đĩa mạng hoặc trên một ổ đĩa di động không có đặc quyền ghi).
- Hành động được chọn trong mục **Hành động khi phát hiện nguy hiểm** cho các tác vụ quét là **Thông báo**, và người dùng đã chọn hành động **Bỏ qua** khi một thông báo về tập tin bị nhiễm được hiển thị.

Bạn có thể bắt đầu thủ công một tác vụ Quét Tùy chỉnh cho các tập tin trong danh sách tập tin chưa được xử lý sau khi cập nhật cơ sở dữ liệu và mô-đun ứng dụng. Trạng thái tập tin có thể thay đổi sau khi quét. Bạn có thể thực hiện hành động cần thiết trên tập tin, tùy thuộc vào trạng thái của chúng.

Ví dụ, bạn có thể thực hiện các hành động sau:

- Xóa các tập tin có trạng thái *Bị nhiễm*.
- Khôi phục các tập tin bị nhiễm có chứa thông tin quan trọng và khôi phục các tập tin được đánh dấu là *Đã khử nhiễm* hoặc *Không nhiễm*.
- Cách ly các tập tin có trạng thái *Có khả năng bị nhiễm*.

Quản lý danh sách các tập tin chưa được xử lý

Danh sách các tập tin chưa được xử lý sẽ xuất hiện dưới dạng một bảng.

Bạn có thể thực hiện các hành động sau với các tập tin chưa được xử lý:

- Xem danh sách các tập tin chưa được xử lý.
- Quét các tập tin chưa được xử lý bằng phiên bản cơ sở dữ liệu và mô-đun hiện tại của Kaspersky Endpoint Security.
- Khôi phục các tập tin từ danh sách các tập tin chưa được xử lý đến thư mục gốc của chúng, hoặc đến một thư mục khác do bạn lựa chọn (khi không thể ghi vào thư mục gốc).
- Loại bỏ các tập tin khỏi danh sách tập tin chưa được xử lý.
- Mở thư mục ban đầu của tập tin chưa được xử lý.

Bạn cũng có thể thực hiện các hành động sau khi quản lý dữ liệu trong bảng:

- Lọc các sự kiện tập tin chưa được xử lý theo giá trị cột hoặc điều kiện lọc tùy chỉnh.
- Sử dụng chức năng tìm kiếm sự kiện tập tin chưa được xử lý.
- Sắp xếp sự kiện tập tin chưa được xử lý.
- Thay đổi thứ tự và nhóm cột được hiển thị trong danh sách các tập tin chưa được xử lý.
- Ghép nhóm các sự kiện tập tin chưa được xử lý.

Bạn có thể sao chép sự kiện tập tin chưa được xử lý được chọn vào bảng nháp, nếu cần thiết.

Bắt đầu một tác vụ Quét Tùy chỉnh cho các tập tin chưa được xử lý

Bạn có thể bắt đầu một tác vụ Quét Tùy chỉnh cho các tập tin chưa được xử lý một cách thủ công. Bạn có thể bắt đầu tác vụ quét nếu, chẳng hạn, tác vụ quét gần nhất đã bị gián đoạn vì một lý do nào đó, hoặc nếu bạn muốn quét lại các tập tin chưa được xử lý sau lần cập nhật cơ sở dữ liệu và các mô-đun ứng dụng mới nhất.

Để bắt đầu một tác vụ Quét Tùy chỉnh cho các tập tin chưa được xử lý:

1. Mở cửa sổ chính của ứng dụng.
2. Ở phần trên của cửa sổ chính của ứng dụng, nhấn vào liên kết **Cách ly** để mở cửa sổ **Lưu trữ**.
3. Trong cửa sổ **Lưu trữ**, chọn thẻ **Các tập tin chưa được xử lý**.
4. Trong bảng ở trên thẻ **Các tập tin chưa được xử lý**, chọn một hoặc nhiều sự kiện liên quan đến các tập tin mà bạn muốn quét.

   Để chọn nhiều sự kiện, giữ nút **CTRL** khi chọn chúng.
5. Bắt đầu tác vụ Quét Tùy chỉnh bằng một trong các cách sau:
   - Nhấn nút **Quét lại**.
   - Nhấn phải chuột để gọi menu ngữ cảnh và chọn **Quét lại**.

Xóa các tập tin trong danh sách tập tin chưa được xử lý

Để xóa các tập tin khỏi danh sách tập tin chưa được xử lý:

1. Mở cửa sổ chính của ứng dụng.
2. Ở phần trên của cửa sổ chính của ứng dụng, nhấn vào liên kết **Cách ly** để mở cửa sổ **Lưu trữ**.
3. Trong cửa sổ **Lưu trữ**, chọn thẻ **Các tập tin chưa được xử lý**.
4. Trong bảng ở trên thẻ **Các tập tin chưa được xử lý**, chọn một hoặc nhiều sự kiện liên quan đến các tập tin mà bạn muốn xóa.

   Để chọn nhiều sự kiện, giữ nút **CTRL** khi chọn chúng.
5. Xóa các tập tin bằng một trong các cách sau:
   - Nhấn nút **Gỡ bỏ**.
   - Nhấn phải chuột để mở menu ngữ cảnh và chọn **Xóa**.

Quét lỗ hổng bảo mật

Mục này chứa thông tin về chi tiết và cấu hình của tác vụ Quét lỗ hổng bảo mật, cùng chỉ dẫn để quản lý danh sách các lỗ hổng bảo mật được phát hiện bởi Kaspersky Endpoint Security khi đang chạy tác vụ Quét lỗ hổng bảo mật.

Xem thông tin về lỗ hổng bảo mật của các ứng dụng đang chạy

Thông tin về lỗ hổng bảo mật của các ứng dụng đang chạy có thể được cung cấp nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Microsoft Windows cho máy trạm. Thông tin này không thể được cung cấp nếu Kaspersky Endpoint Security được cài đặt trên một máy tính chạy Microsoft Windows cho máy chủ tập tin.

Để xem thông tin về lỗ hổng bảo mật của các ứng dụng đang chạy:

1. Mở cửa sổ chính của ứng dụng.
2. Chọn thẻ **Bảo vệ và Kiểm soát**.
3. Mở mục **Bảng kiểm soát**.
4. Nhấn nút **Giám sát Hoạt động Ứng dụng**.

   Cửa sổ **Kiểm soát Đặc quyền Ứng dụng** sẽ được mở ra trên thẻ **Giám sát Hoạt động Ứng dụng**. Bảng **Giám sát Hoạt động Ứng dụng** hiển thị thông tin tóm tắt về hoạt động của các ứng dụng đang chạy trong hệ điều hành. Mức độ nghiêm trọng của lỗ hổng bảo mật của các ứng dụng đang chạy như được xác định bởi thành phần Giám sát Lỗ hổng bảo mật sẽ được hiển thị trong cột **Độ nghiêm trọng của lỗ hổng bảo mật**.

Thông tin về tác vụ Quét lỗ hổng bảo mật

Lỗ hổng bảo mật trong hệ điều hành có thể bị gây ra bởi lỗi lập trình hoặc thiết kế, mật khẩu yếu hoặc hoạt động của phần mềm độc hại. Khi quét để tìm lỗ hổng bảo mật, ứng dụng sẽ phân tích hệ điều hành và tìm kiếm các yếu tố bất thường và cấu hình bị hỏng của các ứng dụng từ Microsoft và các nhà cung cấp khác.

Một tác vụ quét lỗ hổng bảo mật sẽ chẩn đoán bảo mật cho hệ điều hành và phát hiện các tính năng phần mềm có thể được sử dụng bởi kẻ xâm nhập để phát tán các đối tượng độc hại và nhận quyền truy cập đến thông tin cá nhân.

Sau khi tác vụ Quét lỗ hổng bảo mật được bắt đầu, tiến trình hoàn tất của nó sẽ được hiển thị trong trường cạnh tên của **Quét lỗ hổng bảo mật**trong mục **Tác vụ** trên thẻ **Bảo vệ và Kiểm soát** của cửa sổ chính của Kaspersky Endpoint Security.

Kết quả của tác vụ Quét lỗ hổng bảo mật được ghi lại trong báo cáo.

Bắt đầu hoặc dừng tác vụ Quét lỗ hổng bảo mật

Bất kể chế độ chạy được chọn cho tác vụ Quét lỗ hổng bảo mật, bạn có thể bắt đầu hoặc dừng nó bất cứ lúc nào.

Để bắt đầu hoặc dừng tác vụ Quét lỗ hổng bảo mật:

1. Mở cửa sổ chính của ứng dụng.
2. Chọn thẻ **Bảo vệ và Kiểm soát**.
3. Nhấn vào mục **Tác vụ**.

   Mục **Tác vụ** sẽ được mở ra.
4. Nhấn phải chuột để hiển thị menu ngữ cảnh của dòng có chứa tên tác vụ Quét lỗ hổng bảo mật.

   Một menu của tác vụ Quét lỗ hổng bảo mật sẽ được mở ra.
5. Thực hiện một trong các thao tác sau:

   - Để bắt đầu tác vụ Quét lỗ hổng bảo mật, chọn **Bắt đầu quét** từ menu.

     Trạng thái tiến độ tác vụ được hiển thị ở bên phải của nút với tên của tác vụ Quét lỗ hổng bảo mật này sẽ được chuyển thành *Đang chạy*.
   - Để dừng tác vụ Quét lỗ hổng bảo mật, chọn **Dừng quét** từ menu.

     Trạng thái tiến độ tác vụ được hiển thị ở bên phải của nút với tên của tác vụ Quét lỗ hổng bảo mật này sẽ được chuyển thành *Đã dừng*.

Thiết lập cấu hình Quét lỗ hổng bảo mật

Để thiết lập cấu hình của Quét lỗ hổng bảo mật, bạn có thể thực hiện các hành động sau:

- Tạo phạm vi Quét lỗ hổng bảo mật.

  Bạn có thể mở rộng hoặc thu hẹp phạm vi quét bằng cách bổ sung hoặc xóa các ứng dụng được quét để phát hiện lỗ hổng bảo mật.
- Chọn chế độ chạy cho tác vụ Quét lỗ hổng bảo mật.

  Nếu không thể chạy tác vụ vì bất cứ lý do gì (ví dụ, máy tính đang tắt tại thời điểm đó), bạn có thể thiết lập tác vụ bị bỏ qua được tự động bắt đầu ngay khi có thể.
- Thiết lập tác vụ để chạy theo quyền của một tài khoản người dùng khác.

  Theo mặc định, một tác vụ quét được chạy với sự cho phép của tài khoản mà người dùng sử dụng để đăng nhập vào hệ điều hành. Tuy nhiên, bạn có thể cần chạy một tác vụ quét với một tài khoản người dùng khác. Bạn có thể quy định một người dùng có quyền phù hợp trong cấu hình của tác vụ và chạy tác vụ bằng tài khoản của người dùng này.

Tạo phạm vi quét lỗ hổng bảo mật

Một phạm vi quét lỗ hổng bảo mật là một nhà cung cấp phần mềm hoặc đường dẫn đến thư mục đã cài đặt phần mềm (ví dụ, tất cả các ứng dụng Microsoft được cài đặt đến thư mục Program Files).

Để tạo một phạm vi quét lỗ hổng bảo mật:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Tác vụ được lập lịch**, chọn **Quét lỗ hổng bảo mật**.
   Cấu hình tác vụ Quét lỗ hổng bảo mật sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Trong mục **Phạm vi quét**:
   a. Để sử dụng Kaspersky Endpoint Security và tìm kiếm lỗ hổng bảo mật trong các ứng dụng Microsoft được cài đặt trên máy tính, chọn hộp kiểm **Microsoft**.
   b. Để sử dụng Kaspersky Endpoint Security và tìm kiếm lỗ hổng bảo mật trong tất cả các ứng dụng ngoài Microsoft được cài đặt trên máy tính, chọn hộp kiểm **Nhà cung cấp khác**.
   c. Trong cửa sổ **Khu vực quét lỗ hổng bảo mật bổ sung**, nhấn nút **Cấu hình**.
      Cửa sổ **Phạm vi quét lỗ hổng bảo mật** sẽ được mở ra.
   d. Tạo phạm vi quét lỗ hổng bảo mật. Để làm điều này, sử dụng các nút **Thêm** và **Gỡ bỏ**.
   e. Trong cửa sổ **Phạm vi quét lỗ hổng bảo mật**, nhấn nút **OK**.
4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Chọn chế độ chạy cho tác vụ Quét lỗ hổng bảo mật

Để chọn chế độ chạy cho tác vụ Quét lỗ hổng bảo mật:

1. Mở cửa sổ cấu hình ứng dụng.
2. Trong phần bên trái của cửa sổ, trong mục **Tác vụ được lập lịch**, chọn **Quét lỗ hổng bảo mật**.
   Cấu hình tác vụ Quét lỗ hổng bảo mật sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Nhấn nút **Chế độ chạy**.
   Việc này sẽ mở ra thẻ **Chế độ chạy** trong cửa sổ **Quét lỗ hổng bảo mật**.
4. Trong mục **Chế độ chạy**, chọn một tùy chọn chế độ chạy sau đây để bắt đầu tác vụ Quét lỗ hổng bảo mật:
   - Nếu bạn muốn khởi động thủ công tác vụ Quét lỗ hổng bảo mật, chọn **Thủ công**.
   - Nếu bạn muốn thiết lập một lịch khởi động tác vụ Quét lỗ hổng bảo mật, chọn **Theo lập lịch**.
5. Thực hiện một trong các thao tác sau:
   - Nếu bạn đã chọn **Thủ công**, đến bước 6 trong chỉ dẫn này.
   - Nếu bạn đã chọn mục **Theo lập lịch**, hãy quy định cấu hình khởi động cho tác vụ Quét lỗ hổng bảo mật. Để làm điều này:
     a. Trong danh sách thả xuống **Tần suất**, quy định khi nào thì chạy tác vụ Quét lỗ hổng bảo mật. Chọn một trong các tùy chọn sau: **Ngày**, **Mỗi tuần**, **Vào một thời điểm được chỉ định**, **Mỗi tháng**, **Sau khi ứng dụng khởi động**, hoặc **Sau mỗi lần cập nhật**.

b. Tùy thuộc vào các mục được chọn từ danh sách thả xuống **Tần suất**, quy định giá trị cho cấu hình xác định thời gian khởi động tác vụ Quét lỗ hổng bảo mật.

c. Nếu bạn muốn Kaspersky Endpoint Security bắt đầu các tác vụ Quét lỗ hổng bảo mật bị lỡ ngay khi có thể, chọn hộp kiểm **Chạy các tác vụ đã bị bỏ qua**.

> Nếu các đề mục **Sau khi ứng dụng khởi động** hoặc **Sau mỗi lần cập nhật** được chọn từ danh sách thả xuống **Tần suất**, hộp kiểm **Chạy các tác vụ đã bị bỏ qua** sẽ không thể được sử dụng.

6. Nhấn **OK**.

7. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Bắt đầu tác vụ Quét lỗ hổng bảo mật sử dụng các quyền của một tài khoản người dùng khác

Theo mặc định, tác vụ Quét lỗ hổng bảo mật sẽ được bắt đầu bằng tài khoản mà người dùng đã sử dụng để đăng nhập vào hệ điều hành. Tuy nhiên, bạn có thể cần bắt đầu tác vụ Quét lỗ hổng bảo mật với một tài khoản người dùng khác. Bạn có thể quy định một người dùng có các quyền phù hợp trong cấu hình của tác vụ Quét lỗ hổng bảo mật và chạy tác vụ Quét lỗ hổng bảo mật bằng tài khoản của người dùng này.

Để thiết lập việc khởi chạy một tác vụ Quét lỗ hổng bảo mật bằng tài khoản của một người dùng khác:

1. Mở cửa sổ cấu hình ứng dụng.

2. Trong phần bên trái của cửa sổ, trong mục **Tác vụ được lập lịch**, chọn **Quét lỗ hổng bảo mật**.
   Cấu hình tác vụ Quét lỗ hổng bảo mật sẽ được hiển thị ở phần bên phải của cửa sổ.

3. Nhấn nút **Chế độ chạy**.
   Việc này sẽ mở ra thẻ **Chế độ chạy** trong cửa sổ **Quét lỗ hổng bảo mật**.

4. Trên thẻ **Chế độ chạy**, trong mục **Người dùng**, chọn hộp kiểm **Chạy tác vụ như**.

5. Trong trường **Tên**, nhập tên tài khoản của người dùng có các quyền cần thiết để chạy tác vụ Quét lỗ hổng bảo mật.

6. Trong trường **Mật khẩu**, nhập mật khẩu của người dùng có các quyền cần thiết để chạy tác vụ Quét lỗ hổng bảo mật.

7. Nhấn **OK**.

8. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Quản lý danh sách các lỗ hổng bảo mật

Khi quản lý danh sách các lỗ hổng bảo mật, bạn có thể thực hiện các hành động sau:

- Xem danh sách các lỗ hổng bảo mật.
- Bắt đầu tác vụ Quét lỗ hổng bảo mật một lần nữa sau khi cập nhật cơ sở dữ liệu và các mô-đun ứng dụng.
- Xem thông tin chi tiết về lỗ hổng bảo mật và các cách để sửa nó trong một phần riêng.
- Ẩn các đề mục được chọn trong danh sách các lỗ hổng bảo mật.
- Lọc danh sách các lỗ hổng bảo mật theo cấp độ quan trọng.
- Lọc danh sách các lỗ hổng bảo mật theo các giá trị trạng thái *Đã sửa* và *Ẩn*.

Bạn cũng có thể thực hiện các hành động sau khi quản lý dữ liệu trong bảng:

- Lọc danh sách các lỗ hổng bảo mật theo giá trị cột hoặc theo điều kiện bộ lọc tùy chỉnh.
- Sử dụng chức năng tìm kiếm lỗ hổng bảo mật.
- Sắp xếp các đề mục trong danh sách các lỗ hổng bảo mật.
- Thay đổi thứ tự và sắp xếp các cột được hiển thị trong danh sách các lỗ hổng bảo mật.
- Ghép chung các đề mục trong danh sách các lỗ hổng bảo mật.

Thông tin về danh sách các lỗ hổng bảo mật

Kaspersky Endpoint Security sẽ ghi lại kết quả của tác vụ Quét lỗ hổng bảo mật trong danh sách các lỗ hổng bảo mật.

Sau khi bạn đã xem lại các lỗ hổng bảo mật cụ thể và thực hiện hành động được khuyến nghị để khắc phục chúng, Kaspersky Endpoint Security sẽ thay đổi trạng thái của lỗ hổng bảo mật sang *Đã sửa*.

Nếu bạn không muốn hiển thị các đề mục về những lỗ hổng bảo mật cụ thể trong danh sách các lỗ hổng bảo mật, bạn có thể ẩn chúng. Kaspersky Endpoint Security sẽ gán trạng thái *Ẩn* cho các lỗ hổng bảo mật đó.

Danh sách các lỗ hổng bảo mật sẽ xuất hiện dưới dạng một bảng. Mỗi hàng trong bảng đều chứa các thông tin sau đây:

- Một biểu tượng thể hiện cấp độ nghiêm trọng của lỗ hổng bảo mật. Có các cấp độ nghiêm trọng cho lỗ hổng bảo mật sau đây:
  - Biểu tượng . **Thiết yếu**. Mức độ nghiêm trọng này được áp dụng cho các lỗ hổng bảo mật đặc biệt nghiêm trọng, cần được khắc phục ngay lập tức. Kẻ xâm nhập sẽ chủ động khai thác các lỗ hổng bảo mật thuộc cấp này để lây nhiễm cho hệ điều hành của máy tính, hoặc truy cập dữ liệu cá nhân của người dùng. Kaspersky khuyến nghị bạn thực hiện ngay tất cả các bước cần thiết để khắc phục những lỗ hổng bảo mật thuộc cấp độ nghiêm trọng "Thiết yếu".
  - Biểu tượng . **Quan trọng**. Mức độ nghiêm trọng này được áp dụng cho các lỗ hổng bảo mật quan trọng cần sớm được khắc phục. Kẻ xâm nhập có thể chủ động khai thác các lỗ hổng bảo mật thuộc cấp độ này. Kẻ xâm nhập hiện đang không chủ động khai thác các lỗ hổng bảo mật thuộc cấp độ nghiêm trọng "Quan trọng". Kaspersky khuyến nghị bạn thực hiện ngay tất cả các bước cần thiết để khắc phục những lỗ hổng bảo mật thuộc cấp độ nghiêm trọng "Quan trọng".

- Biểu tượng . **Cảnh báo**. Mức độ nghiêm trọng này được áp dụng cho các lỗ hổng bảo mật mà việc khắc phục có thể được tạm hoãn. Tuy nhiên, các lỗ hổng bảo mật này có thể gây nguy hiểm cho bảo mật máy tính trong tương lai.

- ID lỗ hổng bảo mật.
- Tên của ứng dụng mà trong đó phát hiện lỗ hổng bảo mật.
- Mô tả ngắn gọn về lỗ hổng bảo mật.
- Thông tin về nhà phát hành phần mềm như được ghi trong chữ ký điện tử.
- Kết quả của hành động được thực hiện để khắc phục lỗ hổng bảo mật.

Bắt đầu tác vụ Quét lỗ hổng bảo mật một lần nữa

Để cập nhật thông tin về các lỗ hổng bảo mật đã được phát hiện từ trước, bạn có thể khởi động lại tác vụ Quét lỗ hổng bảo mật. Bạn có thể sẽ cần khởi động lại tác vụ quét nếu tác vụ quét lỗ hổng bảo mật trước đó đã bị gián đoạn vì bất cứ lý do nào hoặc nếu bạn muốn quét lại máy tính để phát hiện lỗ hổng bảo mật sau lần cập nhật cơ sở dữ liệu và mô-đun ứng dụng gần nhất.

Để bắt đầu tác vụ Quét lỗ hổng bảo mật một lần nữa:

1. Mở cửa sổ chính của ứng dụng.
2. Ở phần trên của cửa sổ chính của ứng dụng, nhấn vào liên kết **Cách ly** để mở cửa sổ **Lưu trữ**.
3. Trong cửa sổ **Lưu trữ**, chọn thẻ **Lỗ hổng bảo mật**.

   Thẻ **Lỗ hổng bảo mật** chứa danh sách các lỗ hổng bảo mật mà Kaspersky Endpoint Security đã phát hiện trong tác vụ Quét lỗ hổng bảo mật.
4. Ở góc phải dưới của cửa sổ **Lưu trữ**, nhấn nút **Quét lại**.

Kaspersky Endpoint Security sẽ cập nhật thông tin chi tiết về các lỗ hổng bảo mật trong danh sách các lỗ hổng bảo mật.

Trạng thái của một lỗ hổng bảo mật đã được khắc phục qua việc cài đặt bản vá được đề xuất sẽ không thay đổi sau một tác vụ quét lỗ hổng bảo mật khác.

Sửa lỗ hổng bảo mật

Bạn có thể sửa một lỗ hổng bảo mật bằng cách cài đặt một bản cập nhật hệ điều hành, thay đổi thiết lập ứng dụng hoặc cài đặt một bản vá ứng dụng.

Các lỗ hổng bảo mật đã được phát hiện có thể không phải là của những ứng dụng đã cài đặt, mà là bản sao của chúng. Một bản vá chỉ có thể sửa một lỗ hổng bảo mật nếu ứng dụng được cài đặt.

Để sửa một lỗ hổng bảo mật:

1. Mở cửa sổ chính của ứng dụng.

2. Ở phần trên của cửa sổ chính của ứng dụng, nhấn vào liên kết **Cách ly** để mở cửa sổ **Lưu trữ**.

3. Trong cửa sổ **Lưu trữ**, chọn thẻ **Lỗ hổng bảo mật**.

   Thẻ **Lỗ hổng bảo mật** chứa danh sách các lỗ hổng bảo mật mà Kaspersky Endpoint Security đã phát hiện trong tác vụ Quét lỗ hổng bảo mật.

4. Trong danh sách các lỗ hổng bảo mật, chọn mục tương ứng với lỗ hổng bảo mật liên quan.

   Một phần chứa thông tin về lỗ hổng bảo mật cùng khuyến nghị cách khắc phục nó sẽ được mở ra ở cuối danh sách các lỗ hổng bảo mật.

   Các thông tin sau đây có sẵn cho mỗi lỗ hổng bảo mật được chọn:

   - Tên của ứng dụng mà trong đó phát hiện lỗ hổng bảo mật.
   - Phiên bản của ứng dụng mà trong đó phát hiện lỗ hổng bảo mật.
   - Cấp độ nghiêm trọng của một lỗ hổng bảo mật.
   - ID lỗ hổng bảo mật.
   - Ngày và thời gian phát hiện lỗ hổng bảo mật gần đây nhất.
   - Khuyến nghị cách sửa lỗ hổng bảo mật (ví dụ, một liên kết đến website có bản cập nhật hệ điều hành hoặc một bản vá ứng dụng).
   - Liên kết đến website có mô tả về lỗ hổng bảo mật.

5. Để xem mô tả chi tiết của lỗ hổng bảo mật, nhấn vào liên kết **Thông tin bổ sung** để mở ra một trang web với mô tả về mối đe dọa liên quan đến lỗ hổng bảo mật được chọn. Website www.secunia.com cho phép bạn tải về bản cập nhật cần thiết cho phiên bản hiện tại của ứng dụng và cài đặt nó.

6. Chọn một trong các cách sau đây để sửa một lỗ hổng bảo mật:

   - Nếu một hoặc nhiều bản vá có thể được sử dụng cho ứng dụng này, hãy cài đặt bản vá cần thiết bằng cách làm theo chỉ dẫn được cung cấp cạnh tên của bản vá.
   - Nếu một bản cập nhật hệ điều hành có thể được sử dụng, hãy cài đặt bản cập nhật cần thiết đó bằng cách làm theo chỉ dẫn được cung cấp cạnh tên của bản cập nhật.

   Lỗ hổng bảo mật sẽ được sửa sau khi bạn đã cài đặt bản vá hoặc bản cập nhật. Kaspersky Endpoint Security sẽ gán cho lỗ hổng bảo mật này một trạng thái thể hiện rằng lỗ hổng bảo mật đã được sửa. Mục về lỗ hổng bảo mật được sửa sẽ được hiển thị bằng màu xám trong danh sách các lỗ hổng bảo mật.

7. Nếu không có thông tin nào về cách để sửa một lỗ hổng bảo mật được cung cấp ở phần bên dưới của cửa sổ, bạn có thể bắt đầu tác vụ Quét lỗ hổng bảo mật một lần nữa sau khi đã cập nhật các cơ sở dữ liệu và mô-đun của Kaspersky Endpoint Security. Bởi Kaspersky Endpoint Security sẽ quét hệ thống để đối chiếu lỗ hổng bảo mật với một cơ sở dữ liệu các lỗ hổng bảo mật, một mục về lỗ hổng bảo mật đã được sửa có thể xuất hiện sau khi ứng dụng đã được cập nhật.

Ẩn các đề mục trong danh sách các lỗ hổng bảo mật

Bạn có thể ẩn một đề mục lỗ hổng bảo mật được chọn. Kaspersky Endpoint Security sẽ gán trạng thái *Ẩn* đến các đề mục được chọn trong danh sách các lỗ hổng bảo mật và đánh dấu nó là đã ẩn. Sau đó bạn có thể lọc danh sách các lỗ hổng bảo mật theo giá trị trạng thái *Ẩn*.

Để ẩn một đề mục trong danh sách các lỗ hổng bảo mật:

1. Mở cửa sổ chính của ứng dụng.
2. Ở phần trên của cửa sổ chính của ứng dụng, nhấn vào liên kết **Cách ly** để mở cửa sổ **Lưu trữ**.
3. Trong cửa sổ **Lưu trữ**, chọn thẻ **Lỗ hổng bảo mật**.

   Thẻ **Lỗ hổng bảo mật** chứa danh sách các lỗ hổng bảo mật mà Kaspersky Endpoint Security đã phát hiện trong tác vụ Quét lỗ hổng bảo mật.
4. Trong danh sách các lỗ hổng bảo mật, chọn mục về lỗ hổng bảo mật mà bạn muốn ẩn.

   Một phần chứa thông tin về lỗ hổng bảo mật cùng khuyến nghị cách khắc phục nó sẽ được mở ra ở cuối danh sách các lỗ hổng bảo mật.
5. Nhấn nút **Ẩn**.

   Kaspersky Endpoint Security sẽ gán trạng thái *Ẩn* cho lỗ hổng bảo mật được lựa chọn. Các đề mục về lỗ hổng bảo mật với trạng thái *Ẩn* sẽ được di chuyển đến cuối danh sách các lỗ hổng bảo mật và được bôi xám.
6. Để ẩn một đề mục của một lỗ hổng bảo mật trong danh sách các lỗ hổng bảo mật, chọn hộp kiểm **Ẩn** ở đầu danh sách.

Lọc danh sách các lỗ hổng bảo mật theo mức độ nghiêm trọng

Để lọc danh sách các lỗ hổng bảo mật theo mức độ nghiêm trọng:

1. Mở cửa sổ chính của ứng dụng.
2. Ở phần trên của cửa sổ chính của ứng dụng, nhấn vào liên kết **Cách ly** để mở cửa sổ **Lưu trữ**.
3. Trong cửa sổ **Lưu trữ**, chọn thẻ **Lỗ hổng bảo mật**.

   Thẻ **Lỗ hổng bảo mật** chứa danh sách các lỗ hổng bảo mật mà Kaspersky Endpoint Security đã phát hiện trong tác vụ Quét lỗ hổng bảo mật. Ba biểu tượng thể hiện mức độ nghiêm trọng của lỗ hổng bảo mật (Cảnh báo, Quan trọng, Thiết yếu) sẽ xuất hiện ở phần trên của danh sách các lỗ hổng bảo mật trong hàng **Hiển thị độ nghiêm trọng**. Bằng cách nhấn vào các biểu tượng này, bạn có thể lọc danh sách các lỗ hổng bảo mật theo mức độ nghiêm trọng.
4. Nhấn vào một, hai hoặc ba biểu tượng thể hiện mức độ nghiêm trọng của lỗ hổng bảo mật. Lỗ hổng bảo mật phù hợp với cấp độ nghiêm trọng được chọn sẽ được hiển thị trong danh sách. Để ngừng hiển thị lỗ hổng bảo mật phù hợp với một cấp độ nghiêm trọng cụ thể trong danh sách, nhấn vào biểu tượng thể hiện cấp độ nghiêm trọng đó một lần nữa. Nếu không có cấp độ nghiêm trọng nào được chọn, danh sách các lỗ hổng bảo mật sẽ trống.

Các điều kiện lọc danh sách các lỗ hổng bảo mật được quy định sẽ được lưu lại sau khi bạn đã đóng cửa sổ **Lưu trữ**.

Lọc danh sách các lỗ hổng bảo mật theo các giá trị trạng thái Đã sửa và Ẩn

Để lọc danh sách các lỗ hổng bảo mật theo các giá trị trạng thái Đã sửa và Ẩn:

1. Mở cửa sổ chính của ứng dụng.
2. Ở phần trên của cửa sổ chính của ứng dụng, nhấn vào liên kết **Cách ly** để mở cửa sổ **Lưu trữ**.
3. Trong cửa sổ **Lưu trữ**, chọn thẻ **Lỗ hổng bảo mật**.

   Thẻ **Lỗ hổng bảo mật** chứa danh sách các lỗ hổng bảo mật mà Kaspersky Endpoint Security đã phát hiện trong tác vụ Quét lỗ hổng bảo mật.
4. Các hộp kiểm thông báo trạng thái của lỗ hổng bảo mật sẽ được hiển thị cạnh cấu hình **Hiển thị lỗ hổng bảo mật**. Để lọc danh sách các lỗ hổng bảo mật theo trạng thái *Đã sửa*, làm các thao tác sau:

   - Để hiển thị các đề mục về những lỗ hổng bảo mật đã được sửa trong danh sách các lỗ hổng bảo mật, chọn hộp kiểm **sửa lỗi**. Các mục về lỗ hổng bảo mật đã được sửa sẽ được bôi xám trong danh sách các lỗ hổng bảo mật.
   - Để ẩn các đề mục về những lỗ hổng bảo mật đã được sửa trong danh sách các lỗ hổng bảo mật, xóa hộp kiểm **sửa lỗi**.
5. Để lọc danh sách các lỗ hổng bảo mật theo trạng thái *Ẩn*, làm các thao tác sau:

   - Để hiển thị các đề mục về những lỗ hổng bảo mật được ẩn trong danh sách các lỗ hổng bảo mật, chọn hộp kiểm **Ẩn**. Các mục về lỗ hổng bảo mật được ẩn sẽ được bôi xám trong danh sách các lỗ hổng bảo mật.
   - Để ẩn các đề mục về những lỗ hổng bảo mật được ẩn trong danh sách các lỗ hổng bảo mật, xóa hộp kiểm **Ẩn**.

Các điều kiện lọc danh sách các lỗ hổng bảo mật được quy định sẽ không được lưu lại sau khi bạn đã đóng cửa sổ **Lưu trữ**.

Kiểm tra tính toàn vẹn của các mô-đun ứng dụng

Mục này chứa thông tin về chi tiết và cấu hình của tác vụ kiểm tra tính toàn vẹn.

Thông tin về tác vụ Kiểm tra Tính Toàn vẹn

Kaspersky Endpoint Security sẽ kiểm tra mô-đun ứng dụng trong thư mục cài đặt ứng dụng để phát hiện hư hỏng hoặc sửa đổi. Nếu một mô-đun ứng dụng có một chữ ký điện tử sai, mô-đun đó sẽ được coi là bị hỏng.

Sau khi tác vụ kiểm tra tính toàn vẹn được bắt đầu, tiến trình hoàn tất của nó sẽ được hiển thị trong trường cạnh tên của các tác vụ trong mục **Tác vụ** trên thẻ **Bảo vệ và Kiểm soát** của cửa sổ chính của Kaspersky Endpoint Security.

Kết quả của tác vụ kiểm tra tính toàn vẹn được ghi lại trong báo cáo.

Bắt đầu hoặc dừng một tác vụ kiểm tra tính toàn vẹn

Bất kể chế độ chạy được chọn, bạn đều có thể bắt đầu hoặc dừng một tác vụ kiểm tra tính toàn vẹn bất cứ lúc nào.

Để bắt đầu hoặc dừng một tác vụ kiểm tra tính toàn vẹn:

1. Mở cửa sổ chính của ứng dụng.
2. Chọn thẻ **Bảo vệ và Kiểm soát**.
3. Mở mục **Tác vụ**.
4. Nhấn phải chuột để gọi menu ngữ cảnh của dòng có chứa tên tác vụ kiểm tra tính toàn vẹn.
5. Thực hiện một trong các thao tác sau:
   - Để bắt đầu tác vụ kiểm tra tính toàn vẹn, chọn **Bắt đầu quét** từ menu ngữ cảnh.

     Trạng thái tiến độ tác vụ được hiển thị ở bên phải của nút với tên của tác vụ này sẽ được chuyển thành *Đang chạy*.
   - Nếu bạn muốn dừng tác vụ kiểm tra tính toàn vẹn, chọn **Dừng quét** từ menu ngữ cảnh.

     Trạng thái tiến độ tác vụ được hiển thị ở bên phải của nút với tên của tác vụ này sẽ được chuyển thành *Đã dừng*.

Chọn chế độ chạy cho tác vụ kiểm tra tính toàn vẹn

Để chọn chế độ chạy cho tác vụ kiểm tra tính toàn vẹn:

1. Mở cửa sổ cấu hình ứng dụng.

2. Trong phần bên trái của cửa sổ, trong mục **Tác vụ được lập lịch**, chọn **Kiểm tra tính toàn vẹn**.

   Cấu hình tác vụ kiểm tra tính toàn vẹn sẽ được hiển thị ở phần bên phải của cửa sổ.

3. Trong mục **Chế độ chạy**, chọn một trong các tùy chọn sau:

   - Nếu bạn muốn khởi chạy thủ công tác vụ kiểm tra tính toàn vẹn, chọn **Thủ công**.
   - Nếu bạn muốn thiết lập một lịch khởi động tác vụ kiểm tra tính toàn vẹn, chọn **Theo lập lịch**.

4. Nếu bạn đã chọn mục **Theo lập lịch** ở bước trước, quy định cấu hình của lịch chạy tác vụ. Để làm điều này:

   a. Trong danh sách thả xuống **Tần suất**, quy định khi nào thì chạy tác vụ kiểm tra tính toàn vẹn. Chọn một trong các tùy chọn sau: **Phút**, **Giờ**, **Ngày**, **Mỗi tuần**, **Vào một thời điểm được chỉ định**, **Mỗi tháng**, hoặc **Sau khi ứng dụng khởi động**.

   b. Tùy thuộc vào các mục được chọn từ danh sách thả xuống **Tần suất**, quy định giá trị cho cấu hình xác định thời gian khởi động tác vụ.

   c. Nếu bạn muốn Kaspersky Endpoint Security bắt đầu tác vụ kiểm tra tính toàn vẹn bị lỡ ngay khi có thể, chọn hộp kiểm **Chạy các tác vụ đã bị bỏ qua**.

   > Nếu các đề mục **Sau khi ứng dụng khởi động**, **Phút**, hoặc **Giờ** được chọn từ danh sách thả xuống **Tần suất**, hộp kiểm **Chạy các tác vụ đã bị bỏ qua** sẽ không thể được sử dụng.

   d. Nếu bạn muốn Kaspersky Endpoint Security tạm ngưng một tác vụ khi tài nguyên máy tính bị hạn chế, chọn hộp kiểm **Chỉ chạy khi máy tính đang rảnh**.

   Tùy chọn lịch này giúp tiết kiệm tài nguyên máy tính.

5. Nhấn **OK**.

6. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Quản lý báo cáo

Mục này mô tả cách bạn có thể thiết lập cấu hình báo cáo và quản lý các báo cáo.

Nguyên tắc quản lý báo cáo

Thông tin về hoạt động của mỗi thành phần Kaspersky Endpoint Security, hiệu quả của mỗi tác vụ quét, tác vụ cập nhật, tác vụ kiểm soát tính toàn vẹn và tác vụ quét lỗ hổng bảo mật, cũng như hoạt động tổng quát của ứng dụng đều được ghi lại trong các báo cáo.

Dữ liệu báo cáo được trình bày dưới dạng bảng chứa một danh sách các sự kiện. Mỗi dòng trong bảng đều chứa thông tin về một sự kiện riêng biệt. Các thuộc tính sự kiện được đặt trong các cột của bảng. Một số cột là các cột ghép, chứa các cột con với thuộc tính bổ sung. Để xem các thuộc tính bổ sung, bạn phải nhấn nút ⊞ cạnh tên của đồ thị. Các sự kiện được ghi lại trong quá trình hoạt động của các thành phần khác nhau, hay hiệu quả của mỗi tác vụ khác nhau đều có các nhóm thuộc tính khác nhau.

Các báo cáo sau có thể được sử dụng:

- Báo cáo **Kiểm toán hệ thống**. Chứa thông tin về các sự kiện xảy ra trong quá trình tương tác giữa người và ứng dụng, và trong quá trình hoạt động tổng quát của ứng dụng, không liên quan đến bất kỳ thành phần hoặc tác vụ cụ thể nào của Kaspersky Endpoint Security.
- Báo cáo **Tất cả các thành phần bảo vệ**. Chứa thông tin về các sự kiện được ghi trong quá trình hoạt động của các thành phần Kaspersky Endpoint Security sau:
  - Chống virus cho tập tin
  - Chống virus cho thư điện tử.
  - Chống virus cho web.
  - Chống virus cho tin nhắn.
  - Giám sát hệ thống.
  - Tường lửa.
  - Ngăn chặn tấn công mạng.
  - Phòng chống Tấn công BadUSB.
- Báo cáo về hoạt động của một thành phần Kaspersky Endpoint Security, hoặc việc thực thi của một tác vụ.
- Báo cáo **Mã hóa**. Chứa thông tin về các sự kiện xảy ra trong quá trình mã hóa và giải mã dữ liệu.

Các báo cáo sử dụng những cấp độ sự kiện quan trọng như sau:

- **Thông tin các sự kiện**. Biểu tượng . Các sự kiện chính thức thường không chứa thông tin quan trọng.
- **Sự kiện quan trọng**. Biểu tượng . Các sự kiện cần được chú ý bởi chúng phản ánh các tình huống quan trọng trong hoạt động của Kaspersky Endpoint Security.

- **Sự kiện quan trọng**. Biểu tượng . Các sự kiện có tầm quan trọng thiết yếu thể hiện các vấn đề trong hoạt động của Kaspersky Endpoint Security, hoặc lỗ hổng bảo mật trong tính năng bảo vệ máy tính của người dùng.

Để xử lý các báo cáo một cách tiện lợi, bạn có thể thay đổi việc trình bày dữ liệu trên màn hình theo các cách sau:

- Lọc danh sách sự kiện theo nhiều tiêu chí khác nhau.
- Sử dụng chức năng tìm kiếm để tìm một sự kiện cụ thể.
- Xem sự kiện được chọn trong một phần riêng.
- Sắp xếp danh sách sự kiện theo mỗi cột báo cáo.
- Hiển thị và ẩn các sự kiện được ghép chung bởi bộ lọc sự kiện.
- Thay đổi thứ tự và sắp xếp các cột được hiển thị trong báo cáo.

Bạn có thể lưu lại một báo cáo được tạo ra một tập tin văn bản nếu cần thiết.

Bạn cũng có thể xóa thông tin báo cáo trên các thành phần và tác vụ của Kaspersky Endpoint Security, được ghép chung thành nhóm. Kaspersky Endpoint Security sẽ xóa tất cả các đề mục của các báo cáo được chọn từ đề mục cũ nhất đến đề mục mới nhất.

Thiết lập cấu hình báo cáo

Bạn có thể thiết lập cấu hình báo cáo bằng các cách sau đây:

- Thiết lập thời gian lưu trữ báo cáo tối đa.

  Thời gian lưu trữ tối đa cho báo cáo về các sự kiện được ghi lại bởi Kaspersky Endpoint Security là 30 ngày. Sau khoảng thời gian đó, Kaspersky Endpoint Security sẽ tự động xóa các mục cũ nhất từ tập tin báo cáo. Bạn có thể hủy bỏ các hạn chế về thời gian hoặc thay đổi thời gian lưu trữ tối đa cho báo cáo.

- Thiết lập kích cỡ tối đa của tập tin báo cáo.

  Bạn có thể quy định kích cỡ tối đa của tập tin chứa báo cáo. Theo mặc định, kích cỡ tối đa của tập tin báo cáo là 1024 MB. Để tránh vượt quá kích cỡ tối đa của tập tin báo cáo, Kaspersky Endpoint Security sẽ tự động xóa các mục cũ nhất từ tập tin báo cáo khi đạt đến kích cỡ tối đa của tập tin báo cáo. Bạn có thể hủy bỏ giới hạn về kích cỡ của tập tin báo cáo hoặc đặt một giá trị khác.

Thiết lập thời gian lưu trữ báo cáo tối đa

Để thay đổi thời gian lưu trữ báo cáo tối đa:

1. Mở cửa sổ cấu hình ứng dụng.
2. Ở phần bên trái của cửa sổ, trong mục **Cấu hình nâng cao**, chọn **Báo cáo và Lưu trữ**.
3. Ở bên phải của cửa sổ, trong mục **Báo cáo tham số**, thực hiện một trong các hành động sau:
   - Để giới hạn thời gian lưu trữ báo cáo, chọn hộp kiểm **Lưu báo cáo không nhiều hơn**. Trong trường cạnh hộp kiểm **Lưu trữ báo cáo không quá**, nhập thời gian lưu trữ báo cáo tối đa.

Thời gian lưu trữ báo cáo tối đa là 30 ngày ở chế độ mặc định.

- Để hủy bỏ giới hạn thời gian lưu trữ báo cáo, xóa hộp kiểm **Lưu báo cáo không nhiều hơn**.

Giới hạn thời gian lưu trữ báo cáo được bật theo mặc định.

4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Thiết lập kích cỡ tối đa của tập tin báo cáo

Để thiết lập kích cỡ tối đa của tập tin báo cáo:

1. Mở cửa sổ cấu hình ứng dụng.
2. Ở phần bên trái của cửa sổ, trong mục **Cấu hình nâng cao**, chọn **Báo cáo và Lưu trữ**.
3. Ở bên phải của cửa sổ, trong mục **Báo cáo tham số**, thực hiện một trong các hành động sau:
   - Để giới hạn kích cỡ tập tin báo cáo, chọn hộp kiểm **Dung lượng tối đa của tập tin**. Trong trường ở bên phải của hộp kiểm **Kích cỡ tối đa của tập tin**, nhập kích cỡ tối đa của tập tin báo cáo.

     Theo mặc định, kích cỡ của tập tin báo cáo được giới hạn ở 1024 MB.
   - Để xóa giới hạn về kích cỡ tập tin báo cáo, xóa hộp kiểm **Dung lượng tối đa của tập tin**.

   Giới hạn kích cỡ của tập tin báo cáo được bật theo mặc định.
4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Xem báo cáo

Để xem báo cáo:

1. Mở cửa sổ chính của ứng dụng.
2. Ở phần trên của cửa sổ chính của ứng dụng, nhấn vào liên kết **Báo cáo** để mở cửa sổ **Báo cáo**.
3. Để tạo báo cáo Tất cả các thành phần bảo vệ, ở phần bên trái của cửa sổ **Báo cáo**, chọn đề mục **Tất cả các thành phần bảo vệ** trong danh sách các thành phần và tác vụ.

   Báo cáo Tất cả các thành phần bảo vệ được hiển thị ở bên phải của cửa sổ, chứa một danh sách các sự kiện trong hoạt động của tất cả các thành phần bảo vệ của Kaspersky Endpoint Security.
4. Để tạo một báo cáo về hoạt động của một thành phần bảo vệ hoặc tác vụ, ở phần bên trái của cửa sổ **Báo cáo**, trong danh sách các thành phần và tác vụ, chọn một thành phần hoặc tác vụ.

   Báo cáo sẽ được hiển thị ở bên phải của cửa sổ, chứa một danh sách các sự kiện trong hoạt động của thành phần hoặc tác vụ được chọn của Kaspersky Endpoint Security.

Ở chế độ mặc định, các sự kiện báo cáo được sắp xếp theo thứ tự giá trị tăng dần trong cột **Ngày sự kiện**.

Xem thông tin sự kiện trong một báo cáo

Bạn có thể xem một tóm tắt chi tiết về mỗi sự kiện trong báo cáo.

Để xem một tóm tắt chi tiết về một sự kiện trong báo cáo:

1. Mở cửa sổ chính của ứng dụng.
2. Ở phần trên của cửa sổ chính của ứng dụng, nhấn vào liên kết **Báo cáo** để mở cửa sổ **Báo cáo**.
3. Ở phần bên trái của cửa sổ, chọn báo cáo liên quan về thành phần hoặc tác vụ.

   Các sự kiện được bao gồm trong phạm vi báo cáo sẽ được hiển thị trong bảng ở phần bên phải của cửa sổ. Để tìm các sự kiện cụ thể trong báo cáo, sử dụng các chức năng bộ lọc, tìm kiếm và sắp xếp.
4. Chọn sự kiện liên quan trong báo cáo.

Một phần với tóm tắt sự kiện sẽ được hiển thị ở phần dưới của cửa sổ.

Lưu một báo cáo ra tập tin

Bạn có thể lưu báo cáo mà bạn đã tạo ra một tập tin trong định dạng văn bản (TXT) hoặc CSV.

Kaspersky Endpoint Security sẽ ghi lại các sự kiện trong báo cáo theo cách chúng được hiển thị trên màn hình: nói cách khác, với cùng một nhóm và trình tự của thuộc tính sự kiện.

Để lưu một báo cáo ra tập tin:

1. Mở cửa sổ chính của ứng dụng.
2. Ở phần trên của cửa sổ chính của ứng dụng, nhấn vào liên kết **Báo cáo** để mở cửa sổ **Báo cáo**.
3. Thực hiện một trong các thao tác sau:

   - Để tạo báo cáo "Tất cả các thành phần bảo vệ", chọn **Tất cả các thành phần bảo vệ** trong danh sách các thành phần và tác vụ.

     Báo cáo "Tất cả các thành phần bảo vệ" sẽ được hiển thị ở bên phải của cửa sổ, chứa một danh sách các sự kiện trong hoạt động của tất cả các thành phần bảo vệ.

   - Để tạo một báo cáo về hoạt động của một thành phần bảo vệ hoặc tác vụ cụ thể, chọn thành phần hoặc tác vụ này trong danh sách các thành phần và tác vụ.

     Báo cáo sẽ được hiển thị ở bên phải của cửa sổ, chứa một danh sách các sự kiện trong hoạt động của thành phần hoặc tác vụ được chọn.
4. Nếu cần, bạn có thể thay đổi việc trình bày dữ liệu trong báo cáo bằng cách:

   - Lọc sự kiện
   - Chạy truy vấn tìm kiếm sự kiện

- Sắp xếp lại các cột
- Sắp xếp các sự kiện

5. Nhấn vào nút **Lưu báo cáo** ở góc phải trên của cửa sổ.
   Một menu ngữ cảnh sẽ được mở ra.
6. Trong menu ngữ cảnh, chọn mã hóa văn bản để lưu tập tin báo cáo: **Lưu dưới dạng ANSI** hoặc **Lưu dưới dạng Unicode**.
   Cửa sổ **Lưu dưới dạng** tiêu chuẩn của Microsoft Office sẽ được mở ra.
7. Trong cửa sổ **Lưu dưới dạng**, quy định thư mục đích để lưu tập tin báo cáo.
8. Trong trường **Tên tập tin**, nhập tên tập tin báo cáo.
9. Trong trường **Kiểu tập tin**, chọn định dạng cần thiết của tập tin báo cáo: TXT hoặc CSV.
10. Nhấp vào nút **Lưu**.

Xóa nội dung báo cáo

Để xem thông tin từ báo cáo:

1. Mở cửa sổ cấu hình ứng dụng.
2. Ở phần bên trái của cửa sổ, trong mục **Cấu hình nâng cao**, chọn **Báo cáo và Lưu trữ**.
3. Ở bên phải của cửa sổ, trong mục **Báo cáo tham số**, nhấn nút **Xóa báo cáo**.
   Cửa sổ **Xóa báo cáo** sẽ được mở ra.
4. Chọn hộp kiểm đối diện các báo cáo mà bạn muốn xóa thông tin:
   - **Tất cả báo cáo**.
   - **Báo cáo bảo vệ chung**. Chứa thông tin về hoạt động của các thành phần Kaspersky Endpoint Security sau:
     - Chống virus cho tập tin
     - Chống virus cho thư điện tử.
     - Chống virus cho web.
     - Chống virus cho tin nhắn.
     - Giám sát hệ thống.
     - Tường lửa.
     - Ngăn chặn tấn công mạng.
     - Phòng chống Tấn công BadUSB.

- **Báo cáo tác vụ quét**. Chứa thông tin về các tác vụ quét đã được hoàn thiện:
  - Quét Toàn bộ
  - Quét Khu vực Thiết yếu
  - Quét Tùy chỉnh
  - Kiểm tra Tính Toàn vẹn.
- **Báo cáo tác vụ cập nhật**. Chứa thông tin về các tác vụ cập nhật đã được hoàn thiện:
- **Báo cáo Tường lửa**. Chứa thông tin về hoạt động của Tường lửa.
- **Báo cáo thành phần kiểm soát**. Chứa thông tin về hoạt động của các thành phần Kaspersky Endpoint Security sau:
  - Kiểm soát Khởi động Ứng dụng.
  - Kiểm soát đặc quyền ứng dụng.
  - Giám sát lỗ hổng bảo mật.
  - Kiểm soát Thiết bị.
  - Kiểm soát Web.
- **Báo cáo mã hóa dữ liệu**.

5. Nhấn **OK**.

Dịch vụ thông báo

Mục này chứa thông tin về dịch vụ thông báo cảnh báo cho người dùng về các sự kiện trong hoạt động của Kaspersky Endpoint Security, và cũng chứa chỉ dẫn để cấu hình các tham số thông báo.

Thông tin về thông báo Kaspersky Endpoint Security

Tất cả các sự kiện xảy ra trong hoạt động của Kaspersky Endpoint Security. Thông báo về các sự kiện này có thể chỉ mang tính thông tin hoặc chứa các thông tin thiết yếu. Ví dụ, các thông báo có thể là về việc cập nhật thành công cơ sở dữ liệu và mô-đun ứng dụng, hoặc ghi lại các lỗi thành phần cần được khắc phục.

Kaspersky Endpoint Security hỗ trợ việc ghi lại thông tin về các sự kiện trong hoạt động của nhật ký ứng dụng Microsoft Windows và/hoặc nhật ký sự kiện của Kaspersky Endpoint Security.

Kaspersky Endpoint Security cung cấp thông báo bằng những cách sau:

- sử dụng thông báo hiện lên trong khu vực thông báo trên thanh tác vụ của Microsoft Windows;
- qua email.

Bạn có thể thiết lập việc gửi thông báo sự kiện. Phương thức gửi thông báo sẽ được thiết lập cho mỗi loại sự kiện.

Thiết lập dịch vụ thông báo

Bạn có thể thực hiện hành động sau để thiết lập dịch vụ thông báo:

- Thiết lập cấu hình của nhật ký sự kiện ở đó Kaspersky Endpoint Security ghi lại các sự kiện.
- Cấu hình cách hiển thị các thông báo trên màn hình.
- Thiết lập việc truyền tải thông báo email.

Khi sử dụng bảng sự kiện để thiết lập dịch vụ thông báo, bạn có thể thực hiện các hành động sau:

- Lọc các sự kiện của dịch vụ thông báo theo giá trị cột hoặc theo điều kiện bộ lọc tùy chỉnh.
- Sử dụng chức năng tìm kiếm cho các sự kiện của dịch vụ thông báo.
- Sắp xếp các sự kiện của dịch vụ thông báo.
- Thay đổi thứ tự và nhóm cột được hiển thị trong danh sách các sự kiện của dịch vụ thông báo.

Thiết lập cấu hình nhật ký sự kiện

Để thiết lập cấu hình nhật ký sự kiện:

1. Mở cửa sổ cấu hình ứng dụng.

2. Ở phần bên trái của cửa sổ, trong mục **Cấu hình nâng cao**, chọn **Báo cáo và Lưu trữ**.

   Phần bên phải của cửa sổ sẽ hiển thị các cấu hình báo cáo và lưu trữ.

3. Trong mục **Thông báo**, nhấn nút **Cấu hình**.

   Việc này sẽ mở ra cửa sổ **Thông báo**.

   Các thành phần và tác vụ của Kaspersky Endpoint Security được hiển thị ở phần bên trái của cửa sổ. Phần bên phải của cửa sổ liệt kê các sự kiện được tạo cho thành phần hoặc tác vụ được chọn.

4. Ở phần bên trái của cửa sổ, chọn thành phần hoặc tác vụ mà bạn muốn thiết lập cấu hình nhật ký sự kiện.

5. Chọn hộp kiểm đối diện các sự kiện liên quan trong các cột **Lưu báo cáo nội bộ** và **Lưu báo cáo vào mục sự kiện của Windows**.

   Các sự kiện có hộp kiểm được chọn trong cột **Lưu báo cáo nội bộ** sẽ được hiển thị trong **Nhật ký ứng dụng và dịch vụ** trong mục **Nhật ký Sự kiện của Kaspersky**. Các sự kiện có hộp kiểm được chọn trong cột **Lưu báo cáo vào mục sự kiện của Windows** sẽ được hiển thị trong **Nhật ký Windows** và trong mục **Ứng dụng**. Để mở nhật ký sự kiện, nhấn **Start** → **Control Panel** → **Administration** → **Event Viewer**.

6. Nhấn **OK**.

7. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Thiết lập việc hiển thị và truyền tải thông báo

Để thiết lập việc hiển thị và truyền tải thông báo:

1. Mở cửa sổ cấu hình ứng dụng.

2. Ở phần bên trái của cửa sổ, trong mục **Cấu hình nâng cao**, chọn **Báo cáo và Lưu trữ**.

   Phần bên phải của cửa sổ sẽ hiển thị các cấu hình báo cáo và lưu trữ.

3. Trong mục **Thông báo**, nhấn nút **Cấu hình**.

   Việc này sẽ mở ra cửa sổ **Thông báo**.

   Các thành phần và tác vụ của Kaspersky Endpoint Security được hiển thị ở phần bên trái của cửa sổ. Phần bên phải của cửa sổ liệt kê các sự kiện được tạo cho thành phần hoặc tác vụ được chọn.

4. Ở phần bên trái của cửa sổ, chọn thành phần hoặc tác vụ mà bạn muốn thiết lập phương thức thông báo.

5. Trong cột **Thông báo trên màn hình**, chọn hộp kiểm cạnh các sự kiện cần thiết.

   Thông tin về các sự kiện được chọn sẽ được hiển thị trên màn hình dưới dạng các thông báo pop-up trong khu vực thông báo trên thanh tác vụ của Microsoft Windows.

6. Trong cột **Thông báo bằng thư điện tử**, chọn hộp kiểm cạnh các sự kiện cần thiết.

   Thông tin về các sự kiện được chọn sẽ được gửi qua email nếu cấu hình gửi thông báo qua email được thiết lập.

7. Nhấn nút **Cấu hình thông báo thư điện tử**.

   Việc này sẽ mở ra cửa sổ **Cấu hình thông báo thư điện tử**.

8. Chọn hộp kiểm **Gửi thông báo sự kiện** để cho phép gửi thông tin về các sự kiện Kaspersky Endpoint Security được chọn trong cột **Thông báo bằng thư điện tử**.
9. Quy định cấu hình gửi thông báo qua email.
10. Nhấn **OK**.
11. Trong cửa sổ **Cấu hình thông báo thư điện tử**, nhấn **OK**.
12. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Thiết lập việc hiển thị cảnh báo về trạng thái ứng dụng trong khu vực thông báo

Để thiết lập việc hiển thị cảnh báo về trạng thái ứng dụng trong khu vực thông báo:

1. Mở cửa sổ cấu hình ứng dụng.
2. Ở phần bên trái của cửa sổ, trong mục **Cấu hình nâng cao**, chọn **Giao diện**.
   Cấu hình của giao diện Kaspersky Endpoint Security sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Trong mục **Cảnh báo**, chọn hộp kiểm đối diện các hạng mục sự kiện mà bạn muốn nhận thông báo trong khu vực thông báo của Microsoft Windows.
4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Khi các sự kiện liên quan đến hạng mục được chọn xảy ra, biểu tượng ứng dụng trong khu vực thông báo sẽ thay đổi đến  hoặc  tùy thuộc vào mức độ nghiêm trọng của cảnh báo.

Quản lý Cách ly và Sao lưu

Mục này mô tả cách bạn có thể thiết lập và quản lý Cách ly và Sao lưu.

Thông tin về Cách ly và Sao lưu

Cách ly là một danh sách các tập tin có khả năng bị nhiễm. *Tập tin có khả năng bị nhiễm* là các tập tin có thể chứa virus hoặc các mối đe dọa khác, hoặc biến thể của các mối đe dọa đó.

Khi Kaspersky Endpoint Security cách ly một tập tin có khả năng bị nhiễm virus, ứng dụng sẽ không sao chép tập tin mà di chuyển tập tin đó: ứng dụng sẽ xóa tập tin khỏi ổ cứng hoặc email, và lưu nó vào một ổ lưu trữ dữ liệu đặc biệt. Các tập tin trong Cách ly sẽ được lưu trong một định dạng đặc biệt và không gây nguy hiểm.

Kaspersky Endpoint Security có thể phát hiện và cách ly một tập tin có khả năng bị nhiễm trong khi chạy một tác vụ quét virus và trong quá trình hoạt động của các thành phần Chống virus cho tập tin, Chống virus cho thư điện tử và Giám sát Hệ thống.

Kaspersky Endpoint Security sẽ đặt các tập tin vào Cách ly trong các trường hợp sau:

- Mã tập tin giống với một chương trình độc hại đã biết nhưng được sửa đổi một phần, hoặc có cấu trúc giống phần mềm độc hại, nhưng không được liệt kê trong cơ sở dữ liệu của Kaspersky Endpoint Security. Trong trường hợp này, tập tin sẽ được đặt trong Cách ly sau một phân tích suy nghiệm bởi Chống virus cho tập tin và Chống virus cho thư điện tử, hoặc trong quá trình quét virus. Phân tích suy nghiệm hiếm khi phát hiện sai.

- Chuỗi hoạt động mà tập tin thực hiện là nguy hiểm. Trong trường hợp này, tập tin sẽ được đặt trong Cách ly sau khi thành phần Giám sát Hệ thống đã phân tích hành vi của nó.

Sao lưu là một danh sách bản sao dự phòng của các tập tin đã bị xóa hoặc sửa đổi trong quá trình khử nhiễm. *Bản sao dự phòng* là một bản sao của tập tin được tạo ở lần đầu tiên khử nhiễm hoặc xóa tập tin này. Các bản sao dự phòng của tập tin được lưu trữ trong một định dạng đặc biệt và không gây nguy hiểm.

Đôi khi, ứng dụng không thể duy trì tính toàn vẹn của tập tin trong quá trình khử nhiễm. Nếu bạn mất một phần hoặc toàn bộ quyền truy cập đến thông tin quan trọng trong một tập tin được khử nhiễm sau quá trình khử nhiễm, bạn có thể cố gắng khôi phục bản sao được khử nhiễm của tập tin đến thư mục gốc của nó.

Có thể là, sau một bản cập nhật cơ sở dữ liệu hoặc mô-đun phần mềm ứng dụng khác, Kaspersky Endpoint Security chắc chắn sẽ có thể xác định mối đe dọa và vô hiệu hóa chúng. Vì vậy, bạn được khuyến nghị nên quét tập tin được cách ly sau mỗi lần cập nhật cơ sở dữ liệu và mô-đun phần mềm ứng dụng.

Thiết lập cấu hình Cách ly và Sao lưu

Kho lưu trữ dữ liệu bao gồm Cách ly và Sao lưu. Bạn có thể thiết lập cấu hình Cách ly và Sao lưu như sau:

- Thiết lập thời gian lưu trữ tối đa cho các tập tin trong Cách ly và các bản sao của tập tin trong Sao lưu.

Thời gian lưu trữ tối đa mặc định cho các tập tin trong Cách ly và các bản sao của tập tin trong Sao lưu là 30 ngày. Khi thời gian lưu trữ tối đa đã kết thúc, Kaspersky Endpoint Security sẽ xóa các tập tin cũ nhất khỏi kho lưu trữ dữ liệu. Bạn có thể hủy bỏ các hạn chế về thời gian hoặc thay đổi thời gian lưu trữ tối đa cho tập tin.

- Bạn có thể thiết lập kích cỡ tối đa của Cách ly và Sao lưu.

  Theo mặc định, kích cỡ tối đa của Cách ly và Sao lưu là 100 MB. Khi kho lưu trữ dữ liệu đạt giới hạn, Kaspersky Endpoint Security sẽ tự động xóa các tập tin cũ nhất từ Cách ly và Sao lưu, để kích cỡ lưu trữ dữ liệu tối đa không bị vượt quá. Bạn có thể hủy bỏ kích cỡ giới hạn của Cách ly và Sao lưu hoặc thay đổi kích cỡ tối đa của chúng.

Thiết lập thời gian lưu trữ tối đa cho các tập tin trong Cách ly và các bản sao của tập tin trong Sao lưu

Để thiết lập thời gian lưu trữ tối đa cho các tập tin trong Cách ly và các bản sao của tập tin trong Sao lưu:

1. Mở cửa sổ cấu hình ứng dụng.
2. Ở phần bên trái của cửa sổ, trong mục **Cấu hình nâng cao**, chọn **Báo cáo và Lưu trữ**.
3. Thực hiện một trong các thao tác sau:
   - Để hạn chế thời gian lưu trữ tập tin cho Cách ly và Sao lưu, trong mục **Cấu hình cách ly và sao lưu** ở bên phải của cửa sổ, chọn hộp kiểm **Lưu đối tượng không nhiều hơn** Ở trường bên phải của hộp kiểm **Lưu trữ các đối tượng trong tối đa**, quy định thời gian lưu trữ tối đa cho các tập tin trong Cách ly và các bản sao của tập tin trong Sao lưu. Thời gian lưu trữ cho các tập tin trong Cách ly và các bản sao của tập tin trong Sao lưu được giới hạn là 30 ngày ở chế độ mặc định.
   - Để hủy bỏ giới hạn thời gian lưu trữ tập tin cho Cách ly và Sao lưu, trong mục **Cấu hình cách ly và sao lưu** ở bên phải của cửa sổ, xóa hộp kiểm **Lưu đối tượng không nhiều hơn**
4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Thiết lập kích cỡ tối đa của Cách ly và Sao lưu

Để thiết lập kích cỡ tối đa của Cách ly và Sao lưu:

1. Mở cửa sổ cấu hình ứng dụng.
2. Ở phần bên trái của cửa sổ, trong mục **Cấu hình nâng cao**, chọn **Báo cáo và Lưu trữ**.
3. Thực hiện một trong các thao tác sau:
   - Nếu bạn muốn giới hạn tổng kích cỡ của Cách ly và Sao lưu, chọn hộp kiểm **Dung lượng tối đa lưu trữ** trong phần bên phải của cửa sổ, trong mục **Cấu hình Cách ly và Sao lưu** và quy định kích cỡ tối đa của Cách ly và Sao lưu trong trường bên phải của hộp kiểm **Dung lượng tối đa lưu trữ**.

     Theo mặc định, kích cỡ lưu trữ tối đa cho dữ liệu trong thư mục Cách ly và các bản sao dự phòng của tập tin là 100 MB.

- Nếu bạn muốn bỏ giới hạn kích cỡ của Cách ly và Sao lưu, xóa hộp kiểm **Dung lượng tối đa lưu trữ** trong phần bên phải của cửa sổ, trong mục **Cấu hình Cách ly và Sao lưu**.

Kích cỡ của Cách ly và Sao lưu là không giới hạn ở chế độ mặc định.

4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Quản lý Cách ly

Kaspersky Endpoint Security sẽ tự động xóa các tập tin thuộc bất cứ trạng thái nào khỏi Cách ly sau khi thời hạn lưu trữ được quy định trong thiết lập của ứng dụng đã trôi qua.

Các hoạt động tập tin sau có thể được sử dụng khi quản lý Cách ly:

- Xem các tập tin bị cách ly bởi Kaspersky Endpoint Security.
- Quét các tập tin có khả năng bị nhiễm bằng phiên bản cơ sở dữ liệu và mô-đun hiện tại của Kaspersky Endpoint Security.
- Khôi phục các tập tin từ Cách ly đến thư mục gốc của chúng.
- Xóa các tập tin khỏi Cách ly.
- Mở thư mục ban đầu của các tập tin này.

Danh sách các tập tin bị cách ly được trình bày dưới dạng bảng.

Bạn cũng có thể thực hiện các hành động sau khi quản lý dữ liệu trong bảng:

- Lọc các tập tin bị cách ly dựa trên các cột và điều kiện lọc tùy chỉnh.
- Sử dụng chức năng tìm kiếm tập tin bị cách ly.
- Sắp xếp các tập tin bị cách ly.
- Thay đổi thứ tự và nhóm cột được hiển thị trong bảng các tập tin bị cách ly.

Bạn có thể sao chép các sự kiện Cách ly được chọn vào bảng nháp. Để chọn nhiều tập tin được cách ly, nhấp chuột phải để mở menu ngữ cảnh của bất kỳ tập tin nào và chọn **Chọn tất cả**. Để bỏ chọn các tập tin mà bạn không muốn quét, nhấn vào chúng khi đang giữ phím **CTRL**.

Bật và tắt tính năng quét các tập tin trong Cách ly sau khi cập nhật

Nếu Kaspersky Endpoint Security phát hiện các dấu hiệu nhiễm virus khi quét một tập tin, nhưng không thể xác định chương trình độc hại cụ thể đã lây nhiễm cho nó, Kaspersky Endpoint Security sẽ di chuyển tập tin này đến Cách ly. Kaspersky Endpoint Security có thể sẽ xác định chắc chắn được mối đe dọa và vô hiệu hóa chúng sau khi đã cập nhật cơ sở dữ liệu và các mô-đun ứng dụng. Bạn có thể bật tính năng quét tự động các tập tin trong Cách ly sau mỗi lần cập nhật cơ sở dữ liệu và mô-đun ứng dụng.

Chúng tôi khuyến nghị bạn thường xuyên quét các tập tin trong Cách ly. Việc quét có thể thay đổi trạng thái của tập tin. Một số tập tin sau đó có thể được khử nhiễm và khôi phục đến vị trí gốc của chúng để bạn có thể tiếp tục sử dụng.

Để bật tính năng quét các tập tin được cách ly sau khi cập nhật:

1. Mở cửa sổ cấu hình ứng dụng.
2. Ở phần bên trái của cửa sổ, trong mục **Cấu hình nâng cao**, chọn **Báo cáo và Lưu trữ**.

   Cấu hình quản lý các báo cáo và lưu trữ sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Trong mục **Cấu hình Cách ly và Sao lưu**, thực hiện một trong những hành động sau:
   - Để bật tính năng quét các tập tin được cách ly sau mỗi lần cập nhật Kaspersky Endpoint Security, chọn hộp kiểm **Quét lại khu vực cách ly sau khi cập nhật**.
   - Để tắt tính năng quét các tập tin được cách ly sau mỗi lần cập nhật Kaspersky Endpoint Security, xóa hộp kiểm **Quét lại khu vực cách ly sau khi cập nhật**.
4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Bắt đầu một tác vụ Quét Tùy chỉnh cho các tập tin trong Cách ly

Sau khi cập nhật cơ sở dữ liệu và các mô-đun phần mềm ứng dụng, Kaspersky Endpoint Security có thể xác định chắc chắn mối đe dọa trong các tập tin được cách ly và vô hiệu hóa chúng. Nếu ứng dụng không được thiết lập để tự động quét các tập tin được cách ly sau mỗi lần cập nhật cơ sở dữ liệu và các mô-đun ứng dụng, bạn có thể bắt đầu thủ công một tác vụ Quét Tùy chỉnh cho các tập tin được cách ly.

Để bắt đầu một tác vụ Quét Tùy chỉnh cho các tập tin được cách ly:

1. Mở cửa sổ chính của ứng dụng.
2. Ở phần trên của cửa sổ chính của ứng dụng, nhấn vào liên kết **Cách ly** để mở cửa sổ **Lưu trữ**.

   Thẻ **Cách ly** của cửa sổ **Lưu trữ** sẽ được mở ra.
3. Trên thẻ **Cách ly**, chọn một hoặc nhiều tập tin có khả năng bị nhiễm mà bạn muốn quét.

   Để chọn nhiều tập tin được cách ly, nhấp chuột phải để mở menu ngữ cảnh của bất kỳ tập tin nào và chọn **Chọn tất cả**. Để bỏ chọn các tập tin mà bạn không muốn quét, nhấn vào chúng khi đang giữ phím **CTRL**.
4. Bắt đầu tác vụ Quét Tùy chỉnh bằng một trong các cách sau:
   - Nhấn nút **Quét lại**.
   - Nhấn phải chuột để gọi menu ngữ cảnh và chọn **Quét lại**.

Khi tác vụ quét được hoàn tất, một thông báo về số lượng tập tin được quét và số mối đe dọa được phát hiện sẽ được hiển thị.

Khôi phục các tập tin từ Cách ly

Để khôi phục các tập tin từ Cách ly:

1. Mở cửa sổ chính của ứng dụng.
2. Ở phần trên của cửa sổ chính của ứng dụng, nhấn vào liên kết **Cách ly** để mở cửa sổ **Lưu trữ**.

   Thẻ **Cách ly** của cửa sổ **Lưu trữ** sẽ được mở ra.
3. Nếu bạn muốn khôi phục tất cả các tập tin được cách ly, chọn **Khôi phục tất cả** từ menu ngữ cảnh của bất kỳ tập tin nào.

   Kaspersky Endpoint Security sẽ khôi phục tất cả tập tin từ Cách ly đến thư mục gốc của chúng.
4. Để khôi phục một hoặc nhiều tập tin được cách ly:

   a. Trên thẻ **Cách ly**, chọn một hoặc nhiều tập tin mà bạn muốn khôi phục từ Cách ly.

   Để chọn nhiều tập tin được cách ly, nhấp chuột phải để mở menu ngữ cảnh của bất kỳ tập tin nào và chọn **Chọn tất cả**. Để bỏ chọn các tập tin mà bạn không muốn quét, nhấn vào chúng khi đang giữ phím **CTRL**.

   b. Khôi phục các tập tin bằng một trong những cách sau:

   - Bấm vào nút **Khôi phục**.
   - Nhấn phải chuột để mở menu ngữ cảnh và chọn **Khôi phục**.

   Kaspersky Endpoint Security sẽ khôi phục các tập tin được chọn đến thư mục gốc của chúng.

Xóa các tập tin khỏi Cách ly

Để xóa các tập tin khỏi Cách ly:

1. Mở cửa sổ chính của ứng dụng.
2. Ở phần trên của cửa sổ chính của ứng dụng, nhấn vào liên kết **Cách ly** để mở cửa sổ **Lưu trữ**.

   Thẻ **Cách ly** của cửa sổ **Lưu trữ** sẽ được mở ra.
3. Nếu bạn muốn xóa tất cả các tập tin khỏi Cách ly, chọn **Xóa tất cả** từ menu ngữ cảnh của bất kỳ tập tin nào.

   Kaspersky Endpoint Security sẽ xóa tất cả tập tin khỏi Cách ly.
4. Để xóa một hoặc nhiều tập tin được cách ly:

   a. Trong bảng ở trên thẻ **Cách ly**, chọn một hoặc nhiều tập tin có khả năng bị nhiễm mà bạn muốn xóa khỏi Cách ly.

   Để chọn nhiều tập tin được cách ly, nhấp chuột phải để mở menu ngữ cảnh của bất kỳ tập tin nào và chọn **Chọn tất cả**. Để bỏ chọn các tập tin mà bạn không muốn quét, nhấn vào chúng khi đang giữ phím **CTRL**.

   b. Xóa các tập tin bằng một trong các cách sau:

   - Nhấn nút **Gỡ bỏ**.
   - Nhấn phải chuột để mở menu ngữ cảnh và chọn **Xóa**.

Kaspersky Endpoint Security sẽ xóa các tập tin được chọn khỏi Cách ly.

Quản lý Sao lưu

Nếu một mã độc được phát hiện trong một tập tin, Kaspersky Endpoint Security sẽ chặn tập tin đó, đặt một bản sao của nó vào Sao lưu, và cố gắng khử nhiễm tập tin đó. Nếu quá trình khử nhiễm tập tin thành công, trạng thái của bản sao dự phòng của tập tin sẽ được chuyển thành *Đã khử nhiễm*. Tập tin sẽ có thể được sử dụng trong thư mục gốc của nó. Nếu một tập tin không thể được khử nhiễm, Kaspersky Endpoint Security sẽ xóa nó khỏi thư mục gốc. Bạn có thể khôi phục tập tin đó từ bản sao dự phòng đến thư mục gốc của nó.

Khi phát hiện một mã độc trong một tập tin thuộc ứng dụng Windows Store, Kaspersky Endpoint Security sẽ ngay lập tức xóa tập tin đó mà không di chuyển một bản sao của nó đến Sao lưu. Bạn có thể khôi phục tính toàn vẹn của ứng dụng Windows Store sử dụng các công cụ phù hợp của hệ điều hành Microsoft Windows 8 (xem *tập tin trợ giúp của Microsoft Windows 8* để biết thêm chi tiết về cách khôi phục ứng dụng Windows Store).

Kaspersky Endpoint Security sẽ tự động xóa các bản sao dự phòng của các tập tin thuộc bất cứ trạng thái nào khỏi Sao lưu sau khi thời hạn lưu trữ được quy định trong thiết lập của ứng dụng đã trôi qua.

Bạn cũng có thể xóa thủ công bất kỳ bản sao nào của một tập tin khỏi Sao lưu.

Danh sách các bản sao dự phòng của tập tin được trình bày dưới dạng bảng.

Trong lúc quản lý Sao lưu, bạn cũng có thể thực hiện các hành động sau với bản sao dự phòng của các tập tin:

- Xem danh sách bản sao dự phòng của các tập tin.
- Khôi phục tập tin từ các bản sao dự phòng đến thư mục gốc của chúng.
- Xóa bản sao dự phòng của tập tin khỏi Sao lưu.

Bạn cũng có thể thực hiện các hành động sau khi quản lý dữ liệu trong bảng:

- Lọc các bản sao dự phòng theo cột, bao gồm theo các điều kiện lọc tùy chỉnh.
- Sử dụng chức năng tìm kiếm bản sao dự phòng.
- Sắp xếp các bản sao dự phòng.
- Thay đổi thứ tự và nhóm cột được hiển thị trong bảng các bản sao dự phòng.

Bạn có thể sao chép các sự kiện Sao lưu được chọn vào bảng nháp. Để chọn nhiều tập tin Sao lưu, nhấp chuột phải để mở menu ngữ cảnh của bất kỳ tập tin nào và chọn **Chọn tất cả**. Để bỏ chọn các tập tin mà bạn không muốn quét, nhấn vào chúng khi đang giữ phím **CTRL**.

Khôi phục các tập tin từ Sao lưu

Để khôi phục các tập tin từ Sao lưu:

1. Mở cửa sổ chính của ứng dụng.
2. Ở phần trên của cửa sổ chính của ứng dụng, nhấn vào liên kết **Cách ly** để mở cửa sổ **Lưu trữ**.
3. Trong cửa sổ **Lưu trữ**, chọn thẻ **Sao lưu**.
4. Nếu bạn muốn khôi phục tất cả các tập tin từ Sao lưu, chọn **Khôi phục tất cả** từ menu ngữ cảnh của bất kỳ tập tin nào.

   Kaspersky Endpoint Security sẽ khôi phục tất cả tập tin từ bản sao dự phòng đến thư mục gốc của chúng.
5. Để khôi phục một hoặc nhiều tập tin từ Sao lưu:

   a. Trong bảng ở trên thẻ **Sao lưu**, chọn một hoặc nhiều tập tin Sao lưu.

   Để chọn nhiều tập tin được cách ly, nhấp chuột phải để mở menu ngữ cảnh của bất kỳ tập tin nào và chọn **Chọn tất cả**. Để bỏ chọn các tập tin mà bạn không muốn quét, nhấn vào chúng khi đang giữ phím **CTRL**.

   b. Khôi phục các tập tin bằng một trong những cách sau:

   - Bấm vào nút **Khôi phục**.
   - Nhấn phải chuột để mở menu ngữ cảnh và chọn **Khôi phục**.

   Kaspersky Endpoint Security sẽ khôi phục tất cả tập tin từ bản sao dự phòng được chọn đến thư mục gốc của chúng.

Xóa bản sao dự phòng của tập tin khỏi Sao lưu

Để xóa bản sao dự phòng của tập tin khỏi Sao lưu:

1. Mở cửa sổ chính của ứng dụng.
2. Ở phần trên của cửa sổ chính của ứng dụng, nhấn vào liên kết **Cách ly** để mở cửa sổ **Lưu trữ**.
3. Trong cửa sổ **Lưu trữ**, chọn thẻ **Sao lưu**.
4. Nếu bạn muốn xóa tất cả các tập tin từ Sao lưu, thực hiện một trong các hành động sau:

   - Trong menu ngữ cảnh của bất kỳ tập tin nào, chọn **Xóa tất cả**.
   - Nhấn nút **Dọn dẹp lưu trữ**.

   Kaspersky Endpoint Security sẽ xóa tất cả bản sao dự phòng của tập tin khỏi Sao lưu.
5. Nếu bạn muốn xóa một hoặc nhiều tập tin khỏi Sao lưu:

   a. Trong bảng ở trên thẻ **Sao lưu**, chọn một hoặc nhiều tập tin Sao lưu.

   Để chọn nhiều tập tin Sao lưu, nhấp chuột phải để mở menu ngữ cảnh của bất kỳ tập tin nào và chọn **Chọn tất cả**. Để bỏ chọn các tập tin mà bạn không muốn quét, nhấn vào chúng khi đang giữ phím **CTRL**.

   b. Xóa các tập tin bằng một trong các cách sau:

- Nhấn nút **Gỡ bỏ**.
- Nhấn phải chuột để mở menu ngữ cảnh và chọn **Xóa**.

Kaspersky Endpoint Security sẽ xóa các bản sao dự phòng được chọn của tập tin khỏi Sao lưu.

Cấu hình nâng cao của ứng dụng

Phần này mô tả các cấu hình nâng cao của Kaspersky Endpoint Security và cách chúng có thể được thiết lập.

Tạo và sử dụng một tập tin thiết lập

Một tập tin thiết lập với cấu hình của Kaspersky Endpoint Security cho phép bạn thực hiện các tác vụ sau:

- Thực hiện cài đặt cục bộ Kaspersky Endpoint Security thông qua dòng lệnh với các cấu hình được thiết lập sẵn.

  Để làm điều này, bạn phải lưu lại tập tin thiết lập trong cùng thư mục đặt gói phân phối.

- Thực hiện cài đặt từ xa Kaspersky Endpoint Security thông qua Kaspersky Security Center với các cấu hình được thiết lập sẵn.

- Di chuyển cấu hình của Kaspersky Endpoint Security từ một máy tính sang máy tính khác.

Để tạo một tập tin thiết lập:

1. Mở cửa sổ cấu hình ứng dụng.

2. Ở phần bên trái của cửa sổ, chọn mục **Cấu hình nâng cao**.

   Cấu hình nâng cao của ứng dụng sẽ được hiển thị ở phần bên phải của cửa sổ.

3. Trong mục **Cấu hình quản lý**, nhấn nút **Lưu**.

   Điều này sẽ mở ra cửa sổ **Vui lòng lựa chọn một tập tin thiết lập** tiêu chuẩn trong Microsoft Windows.

4. Nhập đường dẫn mà bạn muốn lưu lại tập tin thiết lập, và nhập tên của nó.

   > Để sử dụng tập tin thiết lập để cài đặt cục bộ hoặc từ xa Kaspersky Endpoint Security, bạn phải đặt tên cho nó là install.cfg.

5. Nhấp vào nút **Lưu**.

Để nhập cấu hình của Kaspersky Endpoint Security từ một tập tin thiết lập:

1. Mở cửa sổ cấu hình ứng dụng.

2. Ở phần bên trái của cửa sổ, chọn mục **Cấu hình nâng cao**.

   Cấu hình nâng cao của ứng dụng sẽ được hiển thị ở phần bên phải của cửa sổ.

3. Trong mục **Cấu hình quản lý**, nhấn nút **Nạp**.

   Điều này sẽ mở ra cửa sổ **Vui lòng lựa chọn một tập tin thiết lập** tiêu chuẩn trong Microsoft Windows.

4. Nhập đường dẫn đến tập tin thiết lập.

5. Nhấn nút **Mở**.

Tất cả giá trị của cấu hình Kaspersky Endpoint Security sẽ được đặt theo tập tin thiết lập được chọn.

Vùng tin tưởng

Phần này chứa thông tin về vùng tin tưởng và hướng dẫn cách thiết lập loại trừ quét và tạo một danh sách các ứng dụng được tin tưởng.

Thông tin về vùng tin tưởng

Một *vùng tin tưởng* là một danh sách được thiết lập bởi quản trị viên hệ thống, bao gồm các đối tượng và ứng dụng sẽ không được Kaspersky Endpoint Security giám sát hoạt động. Nói một cách khác, nó là một nhóm loại trừ quét.

Quản trị viên sẽ tự tạo vùng tin tưởng, dựa vào các tính năng của các đối tượng được xử lý và các ứng dụng được cài đặt trên máy tính. Bạn có thể sẽ cần bao gồm các đối tượng và ứng dụng trong vùng tin tưởng khi Kaspersky Endpoint Security chặn truy cập đến một đối tượng hoặc ứng dụng nhất định nếu bạn chắc chắn rằng đối tượng hoặc ứng dụng đó là an toàn.

Bạn có thể loại trừ các đối tượng sau đây khỏi bị quét:

- Tập tin thuộc định dạng nhất định
- Tập tin được lựa chọn bởi một mặt nạ
- Các tập tin được lựa chọn
- Thư mục
- Tiến trình ứng dụng

Loại trừ quét

Loại trừ quét là một nhóm các điều kiện mà theo đó Kaspersky Endpoint Security sẽ không quét một đối tượng để phát hiện virus và các mối đe dọa khác.

Loại trừ quét giúp bạn có thể sử dụng an toàn các phần mềm hợp lệ có thể bị khai thác bởi bọn tội phạm để phá hủy máy tính hoặc dữ liệu người dùng. Mặc dù chúng không có chức năng độc hại nào, nhưng các ứng dụng đó vẫn có thể được sử dụng như một thành phần trung gian trong phần mềm độc hại. Các ví dụ của ứng dụng đó bao gồm các công cụ quản trị từ xa, các trình khách IRC, máy chủ FTP, các tiện ích khác nhau để tạm ngưng hoặc che giấu tiến trình, trình keylogger, bẻ khóa mật khẩu và tự động quay số. Các ứng dụng này không được phân loại là virus. Chi tiết về các phần mềm hợp pháp có thể được sử dụng bởi bọn tội phạm để gây thiệt hại máy tính hoặc dữ liệu cá nhân có thể được xem trên website Bách khoa toàn thư về Virus của Kaspersky tại https://encyclopedia.kaspersky.com/knowledge/riskware/.

Các ứng dụng đó có thể bị chặn bởi Kaspersky Endpoint Security. Để chúng không bị chặn, bạn có thể thiết lập loại trừ quét cho các ứng dụng đang được sử dụng. Để làm điều này, hãy bổ sung tên hoặc mặt nạ tên của ứng dụng được liệt kê trong Bách khoa toàn thư về Virus của Kaspersky vào vùng tin tưởng. Ví dụ, có thể bạn thường xuyên sử dụng chương trình Quản trị từ xa. Đây là một ứng dụng truy cập từ xa cho phép bạn kiểm soát một máy tính từ xa. Kaspersky Endpoint Security coi hoạt động này là đáng ngờ và có thể sẽ chặn nó. Để ứng dụng không bị chặn, hãy tạo một loại trừ quét với tên hoặc mặt nạ tên của ứng dụng được liệt kê trong Bách khoa toàn thư về Virus của Kaspersky.

Nếu một ứng dụng thu thập thông tin và gửi nó ra ngoài để xử lý được cài đặt trên máy tính của bạn, Kaspersky Endpoint Security có thể phân loại ứng dụng này là phần mềm độc hại. Để tránh điều này, bạn có thể loại trừ ứng dụng khỏi bị quét bằng cách thiết lập Kaspersky Endpoint Security như được mô tả trong tài liệu này.

Các loại trừ quét có thể được sử dụng bởi những thành phần ứng dụng và tác vụ sau đây, được thiết lập bởi quản trị viên:

- Chống virus cho tập tin
- Chống virus cho thư điện tử.
- Chống virus cho web.
- Kiểm soát đặc quyền ứng dụng.
- Tác vụ quét
- Giám sát hệ thống.

Danh sách các ứng dụng được tin tưởng

Danh sách các ứng dụng được tin tưởng là một danh sách các ứng dụng có tên, hoạt động mạng (bao gồm hoạt động độc hại) và truy cập đến registry hệ thống không bị giám sát bởi Kaspersky Endpoint Security. Theo mặc định, Kaspersky Endpoint Security sẽ quét các đối tượng được mở, thực thi và lưu bởi bất kỳ tiến trình nào và kiểm soát hoạt động của tất cả các ứng dụng và lưu lượng mạng được tạo bởi chúng. Kaspersky Endpoint Security sẽ loại trừ các ứng dụng có trong danh sách các ứng dụng được tin tưởng khỏi tác vụ quét.

Ví dụ, nếu bạn coi các đối tượng được sử dụng bởi ứng dụng Microsoft Windows Notepad là an toàn và không cần được quét, điều đó có nghĩa là bạn tin tưởng ứng dụng này, và có thể thêm Microsoft Windows Notepad vào danh sách các ứng dụng được tin tưởng. Tác vụ quét sau đó sẽ bỏ qua các đối tượng được sử dụng bởi ứng dụng này.

Thêm vào đó, một số hành động được phân loại là đáng ngờ bởi Kaspersky Endpoint Security có thể là an toàn trong ngữ cảnh sử dụng của một số ứng dụng. Ví dụ, việc theo dõi văn bản được nhập từ bàn phím là một tiến trình thường thấy cho các trình thay đổi bố cục bàn phím tự động (ví dụ như Punto Switcher). Để tính đến các đặc điểm của những ứng dụng đó và loại trừ hoạt động của chúng khỏi tác vụ giám sát, chúng tôi khuyến nghị bạn thêm các ứng dụng đó vào danh sách ứng dụng được tin tưởng.

Việc loại trừ các ứng dụng được tin tưởng khỏi tác vụ quét giúp tránh xung đột tương thích giữa Kaspersky Endpoint Security và các chương trình khác (ví dụ, vấn đề quét hai lần lưu lượng mạng của một máy tính thuộc bên thứ ba bởi Kaspersky Endpoint Security và một ứng dụng chống virus khác), đồng thời tăng hiệu năng của máy tính, điều này là vô cùng quan trọng khi sử dụng các ứng dụng mạng.

Cùng lúc đó, các tập tin thực thi và tiến trình của ứng dụng được tin tưởng vẫn sẽ được quét để phát hiện virus và các phần mềm độc hại khác. Một ứng dụng có thể được loại trừ hoàn toàn khỏi tác vụ quét của Kaspersky Endpoint Security bằng cách thêm chúng vào loại trừ quét.

Tạo một loại trừ quét

Kaspersky Endpoint Security sẽ không quét một đối tượng nếu ổ đĩa hoặc thư mục chứa đối tượng này được bao gồm trong phạm vi quét khi khởi động một tác vụ quét. Tuy nhiên, loại trừ quét sẽ không được áp dụng khi một tác vụ quét tùy chỉnh được bắt đầu cho đối tượng cụ thể này.

Để tạo một loại trừ quét:

1. Mở cửa sổ cấu hình ứng dụng.
2. Chọn mục **Bảo vệ Chống virus** ở phía bên trái.
   Cấu hình bảo vệ chống virus sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Trong mục **Loại trừ quét và ứng dụng tin tưởng**, nhấn nút **Cấu hình**.
   Cửa sổ **Vùng tin tưởng** sẽ được mở ra trên thẻ **Loại trừ quét**.
4. Nhấn vào nút **Thêm**.
   Cửa sổ **Loại trừ quét** sẽ được mở ra. Trong cửa sổ này, bạn có thể tạo một quy tắc loại trừ quét sử dụng một hoặc cả hai tiêu chí từ mục **Thuộc tính**.
5. Để loại trừ một tập tin hoặc thư mục khỏi tác vụ quét:
   a. Trong mục **Thuộc tính**, chọn hộp kiểm **Tập tin hoặc thư mục**.
   b. Nhấn vào liên kết **chọn tập tin hoặc thư mục** trong mục **Mô tả loại trừ quét** để mở cửa sổ **Tên của tập tin hoặc thư mục**.
   c. Nhập tên tập tin/thư mục hoặc mặt nạ của tên tập tin/thư mục hoặc chọn tập tin/thư mục trong cây thư mục bằng cách nhấn nút **Duyệt**.
      Trong tên đại diện của một tập tin hoặc thư mục, bạn có thể sử dụng ký tự hoa thị (*) để thay thế bất kỳ nhóm ký tự nào trong tên tập tin.
      Ví dụ, bạn có thể sử dụng tên đại diện để bổ sung các đường dẫn sau:
      - Đường dẫn đến các tập tin đặt trong bất kỳ thư mục nào:
        - Tên đại diện "*.exe" sẽ bao gồm toàn bộ đường dẫn đến các tập tin có phần mở rộng EXE.
        - Tên đại diện "test" sẽ bao gồm toàn bộ đường dẫn đến các tập tin có tên là "test".
      - Đường dẫn đến các tập tin đặt trong một thư mục cụ thể:
        - Tên đại diện "C:\dir*.*" sẽ bao gồm toàn bộ đường dẫn đến các tập tin đặt trong thư mục C:\dir\, nhưng không nằm trong thư mục con của C:\dir\.
        - Tên đại diện "C:\dir*" sẽ bao gồm toàn bộ đường dẫn đến các tập tin đặt trong thư mục C:\dir\, nhưng không nằm trong thư mục con của C:\dir\.
        - Tên đại diện "C:\dir\" sẽ bao gồm toàn bộ đường dẫn đến các tập tin đặt trong thư mục C:\dir\, nhưng không nằm trong thư mục con của C:\dir\.
        - Tên đại diện "C:\dir*.exe" sẽ bao gồm toàn bộ đường dẫn đến các tập tin có phần mở rộng EXE đặt trong thư mục C:\dir\, nhưng không nằm trong thư mục con của C:\dir\.
        - Tên đại diện "C:\dir\test" sẽ bao gồm toàn bộ đường dẫn đến các tập tin có tên là "test" đặt trong thư mục C:\dir\, nhưng không nằm trong thư mục con của C:\dir\.

- Tên đại diện "C:\dir*\test" sẽ bao gồm toàn bộ đường dẫn đến các tập tin có tên là "test" đặt trong thư mục C:\dir\ và trong thư mục con của C:\dir\.

- Đường dẫn đến các tập tin đặt trong tất cả thư mục có tên cụ thể:

  - Tên đại diện "dir*.*" sẽ bao gồm toàn bộ đường dẫn đến các tập tin đặt trong các thư mục có tên là "dir", nhưng không nằm trong thư mục con của các thư mục đó.

  - Tên đại diện "dir*" sẽ bao gồm toàn bộ đường dẫn đến các tập tin đặt trong các thư mục có tên là "dir", nhưng không nằm trong thư mục con của các thư mục đó.

  - Tên đại diện "dir\" sẽ bao gồm toàn bộ đường dẫn đến các tập tin đặt trong các thư mục có tên là "dir", nhưng không nằm trong thư mục con của các thư mục đó.

  - Tên đại diện "dir*.exe" sẽ bao gồm toàn bộ đường dẫn đến các tập tin có phần mở rộng EXE đặt trong các thư mục có tên là "dir", nhưng không nằm trong thư mục con của các thư mục đó.

  - Tên đại diện "dir\test" sẽ bao gồm toàn bộ đường dẫn đến các tập tin có tên là "test" đặt trong các thư mục có tên là "dir", nhưng không nằm trong thư mục con của các thư mục đó.

d. Trong cửa sổ **Tên của tập tin hoặc thư mục**, nhấn **OK**.

Một liên kết đến tập tin hoặc thư mục được bổ sung sẽ xuất hiện trong mục **Mô tả loại trừ quét** của cửa sổ **Loại trừ quét**.

6. Để loại trừ các đối tượng có tên cụ thể khỏi tác vụ quét:

a. Trong mục **Thuộc tính**, chọn hộp kiểm **Tên đối tượng**.

b. Nhấn vào liên kết **nhập tên đối tượng** trong mục **Mô tả loại trừ quét** để mở cửa sổ **Tên đối tượng**.

c. Nhập vào tên hoặc mặt nạ tên đối tượng theo phân loại của Bách khoa toàn thư về Virus của Kaspersky:

d. Nhấn **OK** trong cửa sổ **Tên đối tượng**.

Một liên kết đến tên đối tượng được bổ sung sẽ xuất hiện trong mục **Mô tả loại trừ quét** của cửa sổ **Loại trừ quét**.

7. Nếu cần thiết, trong trường **Bình luận**, nhập một nhận xét ngắn về loại trừ quét mà bạn đang tạo.

8. Quy định thành phần Kaspersky Endpoint Security nên sử dụng loại trừ quét:

a. Nhấn vào liên kết **bất kỳ** trong mục **Mô tả loại trừ quét** để kích hoạt liên kết **chọn thành phần**.

b. Nhấn vào liên kết **lựa chọn thành phần** để mở ra cửa sổ **Thành phần bảo vệ**.

c. Chọn hộp kiểm đối diện các thành phần mà quy tắc loại trừ quét nên được áp dụng.

d. Trong cửa sổ **Thành phần bảo vệ**, nhấn **OK**.

Nếu các thành phần được quy định trong cấu hình của loại trừ quét, quy tắc loại trừ này sẽ chỉ được áp dụng trong quá trình quét của các thành phần Kaspersky Endpoint Security này.

Nếu các thành phần không được quy định trong cấu hình của loại trừ quét, quy tắc loại trừ này được áp dụng trong quá trình quét của tất cả các thành phần Kaspersky Endpoint Security.

9. Trong cửa sổ **Loại trừ quét**, nhấn **OK**.

   Quy tắc loại trừ quét mà bạn vừa thêm sẽ xuất hiện trong bảng trên thẻ **Loại trừ quét** của cửa sổ **Vùng tin tưởng**. Cấu hình được thiết lập của loại trừ quét này sẽ xuất hiện trong mục **Mô tả loại trừ quét**.

10. Trong cửa sổ **Vùng tin tưởng**, nhấn **OK**.

11. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Sửa một loại trừ quét

Để sửa một loại trừ quét:

1. Mở cửa sổ cấu hình ứng dụng.

2. Chọn mục **Bảo vệ Chống virus** ở phía bên trái.
   Cấu hình bảo vệ chống virus sẽ được hiển thị ở phần bên phải của cửa sổ.

3. Trong mục **Loại trừ quét và ứng dụng tin tưởng**, nhấn nút **Cấu hình**.
   Cửa sổ **Vùng tin tưởng** sẽ được mở ra trên thẻ **Loại trừ quét**.

4. Chọn quy tắc loại trừ quét mà bạn muốn sửa trong danh sách.

5. Thay đổi cấu hình loại trừ quét sử dụng một trong các phương thức sau:

   - Nhấn nút **Chỉnh sửa**.
     Cửa sổ **Loại trừ quét** sẽ được mở ra.
   - Mở cửa sổ để sửa cấu hình cần thiết bằng cách nhấn vào liên kết trong trường **Mô tả loại trừ quét**.

6. Nếu bạn đã nhấn nút **Chỉnh sửa** ở bước trước, nhấn **OK** trong cửa sổ **Loại trừ quét**.
   Cấu hình đã được sửa đổi của loại trừ quét này sẽ xuất hiện trong mục **Mô tả loại trừ quét**.

7. Trong cửa sổ **Vùng tin tưởng**, nhấn **OK**.

8. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Xóa một loại trừ quét

Để xóa một loại trừ quét:

1. Mở cửa sổ cấu hình ứng dụng.

2. Chọn mục **Bảo vệ Chống virus** ở phía bên trái.
   Cấu hình bảo vệ chống virus sẽ được hiển thị ở phần bên phải của cửa sổ.

3. Trong mục **Loại trừ quét và ứng dụng tin tưởng**, nhấn nút **Cấu hình**.

Cửa sổ **Vùng tin tưởng** sẽ được mở ra trên thẻ **Loại trừ quét**.

4. Chọn quy tắc loại trừ quét mà bạn cần trong danh sách loại trừ quét.
5. Nhấn nút **Gỡ bỏ**.
   Loại trừ quét đã bị xóa sẽ biến mất khỏi danh sách.
6. Trong cửa sổ **Vùng tin tưởng**, nhấn **OK**.
7. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Bật và tắt một loại trừ quét

Để bật hoặc tắt một quy tắc loại trừ quét:

1. Mở cửa sổ cấu hình ứng dụng.
2. Chọn mục **Bảo vệ Chống virus** ở phía bên trái.
   Cấu hình bảo vệ chống virus sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Trong mục **Loại trừ quét và ứng dụng tin tưởng**, nhấn nút **Cấu hình**.
   Cửa sổ **Vùng tin tưởng** sẽ được mở ra trên thẻ **Loại trừ quét**.
4. Chọn quy tắc loại trừ mà bạn cần trong danh sách loại trừ quét.
5. Thực hiện một trong các thao tác sau:
   - Để bật một quy tắc loại trừ quét, chọn hộp kiểm cạnh tên của quy tắc loại trừ quét đó.
   - Để tắt một quy tắc loại trừ quét, xóa hộp kiểm cạnh tên của quy tắc loại trừ quét đó.
6. Nhấn **OK**.
7. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Sửa danh sách các ứng dụng được tin tưởng

Để danh sách các ứng dụng được tin tưởng:

1. Mở cửa sổ cấu hình ứng dụng.
2. Chọn mục **Bảo vệ Chống virus** ở phía bên trái.
   Cấu hình bảo vệ chống virus sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Trong mục **Loại trừ quét và ứng dụng tin tưởng**, nhấn nút **Cấu hình**.
   Cửa sổ **Vùng tin tưởng** sẽ được mở ra.
4. Trong cửa sổ **Vùng tin tưởng**, chọn thẻ **Ứng dụng được tin tưởng**.

5. Để thêm một ứng dụng vào danh sách các ứng dụng được tin tưởng:

   a. Nhấn vào nút **Thêm**.

   b. Trong menu ngữ cảnh được mở ra, thực hiện một trong các thao tác sau:

   - Nếu bạn muốn tìm một ứng dụng trong danh sách các ứng dụng được cài đặt trên máy tính, chọn mục **Ứng dụng** trong menu.

     Cửa sổ **Lựa chọn ứng dụng** sẽ được mở ra.

   - Nếu bạn muốn quy định đường dẫn đến tập tin thực thi của ứng dụng liên quan, chọn **Duyệt**.

     Cửa sổ **Mở tập tin** tiêu chuẩn trong Microsoft Windows sẽ được mở ra.

   c. Chọn ứng dụng bằng một trong các cách sau:

   - Nếu bạn đã chọn **Ứng dụng** ở bước trước đó, chọn ứng dụng trong danh sách các ứng dụng được cài đặt trên máy tính và nhấn nút **OK** trong cửa sổ **Lựa chọn ứng dụng**.

   - Nếu bạn đã chọn **Duyệt** ở bước trước đó, quy định đường dẫn đến tập tin thực thi của ứng dụng liên quan và nhấn nút **Mở** trong cửa sổ **Mở** tiêu chuẩn của Microsoft Windows.

   Hành động này sẽ mở ra cửa sổ **Loại trừ quét ứng dụng**.

   a. Chọn các hộp kiểm đối diện quy tắc vùng tin tưởng liên quan cho ứng dụng được chọn:

   - **Không quét các tập tin đã mở**.
   - **Không giám sát hoạt động ứng dụng**.
   - **Không kế thừa những hạn chế của tiến trình cha (ứng dụng)**.
   - **Không giám sát hoạt động của ứng dụng con**.
   - **Không chặn tương tác với giao diện ứng dụng**.
   - **Không quét lưu thông mạng**.

   b. Trong cửa sổ **Loại trừ quét ứng dụng**, nhấn **OK**.

   Ứng dụng được tin tưởng mà bạn vừa thêm sẽ xuất hiện trong danh sách các ứng dụng được tin tưởng.

6. Để sửa cấu hình của một ứng dụng được tin tưởng:

   a. Chọn một ứng dụng được tin tưởng trong danh sách các ứng dụng được tin tưởng.

   b. Nhấn nút **Chỉnh sửa**.

   c. Cửa sổ **Loại trừ quét ứng dụng** sẽ được mở ra.

   d. Chọn hoặc xóa các hộp kiểm đối diện quy tắc vùng tin tưởng liên quan cho ứng dụng được chọn:

Nếu không có quy tắc vùng tin tưởng nào được chọn trong cửa sổ **Loại trừ quét ứng dụng**, ứng dụng được tin tưởng sẽ được bao gồm trong tác vụ quét. Trong trường hợp này, ứng dụng được tin tưởng sẽ không bị xóa khỏi danh sách các ứng dụng được tin tưởng, nhưng hộp kiểm của nó sẽ bị xóa.

e. Trong cửa sổ **Loại trừ quét ứng dụng**, nhấn **OK**.

7. Để xóa một ứng dụng được tin tưởng khỏi danh sách các ứng dụng được tin tưởng:

   a. Chọn một ứng dụng được tin tưởng trong danh sách các ứng dụng được tin tưởng.

   b. Nhấn nút **Gỡ bỏ**.

8. Trong cửa sổ **Vùng tin tưởng**, nhấn **OK**.

9. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Bật và tắt quy tắc vùng tin tưởng cho một ứng dụng trong danh sách các ứng dụng được tin tưởng.

Để bật hoặc tắt hành động của một quy tắc vùng tin tưởng được áp dụng cho một ứng dụng từ danh sách các ứng dụng được tin tưởng:

1. Mở cửa sổ cấu hình ứng dụng.

2. Chọn mục **Bảo vệ Chống virus** ở phía bên trái.
   Cấu hình bảo vệ chống virus sẽ được hiển thị ở phần bên phải của cửa sổ.

3. Trong mục **Loại trừ quét và ứng dụng tin tưởng**, nhấn nút **Cấu hình**.
   Cửa sổ **Vùng tin tưởng** sẽ được mở ra.

4. Trong cửa sổ **Vùng tin tưởng**, chọn thẻ **Ứng dụng được tin tưởng**.

5. Trong danh sách các ứng dụng được tin tưởng, chọn ứng dụng được tin tưởng cần thiết.

6. Thực hiện một trong các thao tác sau:

   - Để loại trừ một ứng dụng được tin tưởng khỏi tác vụ quét của Kaspersky Endpoint Security, chọn hộp kiểm cạnh tên của nó.

   - Để bao gồm một ứng dụng được tin tưởng trong tác vụ quét của Kaspersky Endpoint Security, xóa hộp kiểm cạnh tên của nó.

7. Nhấn **OK**.

8. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Sử dụng ổ lưu trữ chứng chỉ hệ thống được tin tưởng

Việc sử dụng kho lưu trữ chứng chỉ hệ thống cho phép bạn loại trừ các ứng dụng có chữ ký điện tử được tin tưởng khỏi các tác vụ quét virus. Kaspersky Endpoint Security sẽ tự động gán các ứng dụng đó vào nhóm *Tin tưởng*.

Để bắt đầu sử dụng kho lưu trữ chứng chỉ hệ thống được tin tưởng:

1. Mở cửa sổ cấu hình ứng dụng.
2. Chọn mục **Bảo vệ Chống virus** ở phía bên trái.
   Cấu hình bảo vệ chống virus sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Trong mục **Loại trừ quét và ứng dụng tin tưởng**, nhấn nút **Cấu hình**.
   Cửa sổ **Vùng tin tưởng** sẽ được mở ra.
4. Trong cửa sổ **Vùng tin tưởng**, chọn thẻ **Cửa hàng chứng nhận hệ thống tin tưởng**.
5. Chọn hộp kiểm **Sử dụng cửa hàng chứng nhận hệ thống tin tưởng**.
6. Trong danh sách thả xuống **Cửa hàng chứng nhận hệ thống tin tưởng**, chọn kho lưu trữ hệ thống sẽ được Kaspersky Endpoint Security coi là tin tưởng.
7. Trong cửa sổ **Vùng tin tưởng**, nhấn **OK**.
8. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Tự bảo vệ cho Kaspersky Endpoint Security

Phần này mô tả tính năng tự bảo vệ và cơ cấu bảo vệ điều khiển từ xa của Kaspersky Endpoint Security, đồng thời hướng dẫn cách để thiết lập cấu hình của các cơ cấu này.

Thông tin về Tự bảo vệ của Kaspersky Endpoint Security

Kaspersky Endpoint Security sẽ bảo vệ máy tính khỏi các chương trình độc hại, bao gồm những phần mềm độc hại cố gắng chặn hoạt động của Kaspersky Endpoint Security, hoặc thậm chí xóa ứng dụng này khỏi máy tính.

Sự ổn định của hệ thống bảo mật trên máy tính sẽ được đảm bảo bởi cơ cấu tự bảo vệ và bảo vệ điều khiển từ xa trong Kaspersky Endpoint Security.

Cơ cấu *Tự bảo vệ* sẽ ngăn chặn việc sửa đổi hoặc xóa các tập tin ứng dụng trên ổ cứng, tiến trình bộ nhớ, và các mục trong registry hệ thống.

Bảo vệ điều khiển từ xa sẽ chặn mọi nỗ lực của một máy tính từ xa để điều khiển các dịch vụ ứng dụng.

Trên các máy tính chạy hệ điều hành 64 bit, chỉ thành phần Tự bảo vệ của Kaspersky Endpoint Security mới có thể chặn việc sửa đổi và xóa các tập tin ứng dụng trên ổ cứng và các mục trong registry hệ thống.

Bật hoặc tắt Tự bảo vệ

Cơ cấu Tự bảo vệ của Kaspersky Endpoint Security được bật theo mặc định. Bạn có thể tắt Tự bảo vệ nếu cần thiết.

Để bật hoặc tắt Tự bảo vệ:

1. Mở cửa sổ cấu hình ứng dụng.
2. Ở phần bên trái của cửa sổ, chọn mục **Cấu hình nâng cao**.
   Cấu hình nâng cao của ứng dụng sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Thực hiện một trong các thao tác sau:
   - Để bật cơ cấu Tự bảo vệ, chọn hộp kiểm **Công nghệ quét**.
   - Để tắt cơ cấu Tự bảo vệ, xóa hộp kiểm **Cho phép Tự bảo vệ**.
4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Bật hoặc tắt Bảo vệ điều khiển từ xa

Cơ cấu bảo vệ điều khiển từ xa được bật theo mặc định. Bạn có thể tắt cơ cấu bảo vệ điều khiển từ xa nếu cần thiết.

Để bật hoặc tắt cơ cấu bảo vệ điều khiển từ xa:

1. Mở cửa sổ cấu hình ứng dụng.
2. Ở phần bên trái của cửa sổ, chọn mục **Cấu hình nâng cao**.
   Cấu hình nâng cao của ứng dụng sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Thực hiện một trong các thao tác sau:
   - Để bật cơ cấu bảo vệ điều khiển từ xa, chọn **Vô hiệu hóa quản lý bên ngoài các dịch vụ hệ thống**.
   - Để tắt cơ cấu bảo vệ điều khiển từ xa, xóa **Vô hiệu hóa quản lý bên ngoài các dịch vụ hệ thống**.
4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Hỗ trợ các ứng dụng quản trị từ xa

Có thể bạn sẽ cần sử dụng một ứng dụng quản trị từ xa trong khi tính năng bảo vệ kiểm soát bên ngoài được bật.

Để cho phép hoạt động của các ứng dụng quản trị từ xa:

1. Mở cửa sổ cấu hình ứng dụng.
2. Chọn mục **Bảo vệ Chống virus** ở phía bên trái.

   Cấu hình bảo vệ chống virus sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Trong mục **Loại trừ quét và ứng dụng tin tưởng**, nhấn nút **Cấu hình**.

   Cửa sổ **Vùng tin tưởng** sẽ được mở ra.
4. Trong cửa sổ **Vùng tin tưởng**, chọn thẻ **Ứng dụng được tin tưởng**.
5. Nhấn vào nút **Thêm**.
6. Trong menu ngữ cảnh được mở ra, thực hiện một trong các thao tác sau:

   - Để tìm ứng dụng quản trị từ xa trong danh sách các ứng dụng được cài đặt trên máy tính, chọn mục **Ứng dụng**.

     Cửa sổ **Lựa chọn ứng dụng** sẽ được mở ra.
   - Để quy định đường dẫn đến tập tin thực thi của ứng dụng quản trị từ xa, chọn **Duyệt**.

     Cửa sổ **Mở tập tin** tiêu chuẩn trong Microsoft Windows sẽ được mở ra.
7. Chọn ứng dụng bằng một trong các cách sau:

   - Nếu bạn đã chọn **Ứng dụng** ở bước trước đó, chọn ứng dụng trong danh sách các ứng dụng được cài đặt trên máy tính và nhấn nút **OK** trong cửa sổ **Lựa chọn ứng dụng**.
   - Nếu bạn đã chọn **Duyệt** ở bước trước đó, quy định đường dẫn đến tập tin thực thi của ứng dụng liên quan và nhấn nút **Mở** trong cửa sổ **Mở** tiêu chuẩn của Microsoft Windows.

   Hành động này sẽ mở ra cửa sổ **Loại trừ quét ứng dụng**.
8. Chọn hộp kiểm **Không giám sát hoạt động ứng dụng**.
9. Trong cửa sổ **Loại trừ quét ứng dụng**, nhấn **OK**.

   Ứng dụng được tin tưởng mà bạn vừa thêm sẽ xuất hiện trong danh sách các ứng dụng được tin tưởng.
10. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Hiệu năng của Kaspersky Endpoint Security và tính tương thích với các ứng dụng khác

Phần này chứa thông tin về hiệu năng của Kaspersky Endpoint Security và tính tương thích với các ứng dụng khác, đồng thời cũng hướng dẫn lựa chọn các loại đối tượng có thể được phát hiện và chế độ hoạt động của Kaspersky Endpoint Security.

Thông tin về hiệu năng của Kaspersky Endpoint Security và tính tương thích với các ứng dụng khác

Hiệu năng của Kaspersky Endpoint Security

Hiệu năng của Kaspersky Endpoint Security đồng nghĩa với số loại đối tượng có thể gây hại cho máy tính có thể được phát hiện, cũng như mức tiêu thụ năng lượng và sử dụng tài nguyên máy tính.

Chọn các loại đối tượng có thể được phát hiện

Kaspersky Endpoint Security cho phép bạn tinh chỉnh chế độ bảo vệ máy tính của mình và chọn các loại đối tượng mà ứng dụng sẽ phát hiện trong quá trình hoạt động. Kaspersky Endpoint Security sẽ luôn quét hệ điều hành để phát hiện virus, sâu và Trojan. Bạn không thể tắt tính năng quét các loại đối tượng này. Các phần mềm độc hại này có thể gây thiệt hại đáng kể đến máy tính. Để bảo mật tốt hơn cho máy tính của mình, bạn có thể mở rộng phạm vi phát hiện loại đối tượng bằng cách bật tính năng giám sát các phần mềm hợp pháp có thể được sử dụng bởi bọn tội phạm để phá hoại máy tính hoặc dữ liệu cá nhân của bạn.

Sử dụng chế độ tiết kiệm năng lượng

Mức tiêu thụ năng lượng bởi ứng dụng là một cân nhắc chính cho các máy tính lưu động. Các tác vụ được lập lịch của Kaspersky Endpoint Security thường sử dụng khá nhiều tài nguyên. Khi máy tính đang chạy bằng pin, bạn có thể sử dụng chế độ tiết kiệm năng lượng để tiêu thụ ít công suất hơn.

Trong chế độ tiết kiệm năng lượng, các tác vụ được lập lịch sau sẽ tự động được hoãn:

- Tác vụ cập nhật
- Tác vụ Quét Toàn bộ
- Tác vụ Quét khu vực quan trọng
- Tác vụ Quét Tùy chỉnh
- Tác vụ Quét lỗ hổng bảo mật
- Tác vụ Kiểm tra Tính Toàn vẹn

Dù chế độ tiết kiệm năng lượng có được bật hay không, Kaspersky Endpoint Security vẫn sẽ tạm ngưng các tác vụ mã hóa khi một máy tính lưu động chuyển sang sử dụng pin. Ứng dụng sẽ khôi phục các tác vụ mã hóa khi máy tính lưu động chuyển từ pin sang nguồn điện chính.

Nhường tài nguyên máy tính cho các ứng dụng khác

Việc sử dụng tài nguyên máy tính của Kaspersky Endpoint Security có thể ảnh hưởng đến hiệu năng của các ứng dụng khác. Để giải quyết vấn đề cùng hoạt động khi CPU và hệ thống con ổ cứng đang chịu tải nặng, Kaspersky Endpoint Security có thể tạm ngưng các tác vụ đã được lập lịch và nhường tài nguyên cho các ứng dụng khác.

Tuy nhiên, một số ứng dụng vẫn sẽ được khởi chạy ngay khi tài nguyên CPU trở nên khả dụng, và tiếp tục hoạt động trong chế độ nền. Để ngăn tác vụ quét khỏi phụ thuộc vào hiệu năng của các ứng dụng khác, bạn không nên nhường tài nguyên hệ điều hành cho chúng.

Bạn có thể bắt đầu các tác vụ đó một cách thủ công, nếu cần thiết.

Sử dụng công nghệ khử nhiễm cao cấp

Các chương trình độc hại ngày nay có thể xâm nhập vào cấp độ sâu nhất của một hệ điều hành, và khiến việc tiêu diệt chúng là gần như không thể. Khi phát hiện hoạt động độc hại trong hệ điều hành, Kaspersky Endpoint Security sẽ thực hiện một quy trình khử nhiễm sâu rộng sử dụng công nghệ khử nhiễm cao cấp. *Công nghệ khử nhiễm cao cấp* nhằm tẩy sạch hệ điều hành và loại trừ các chương trình độc hại đã bắt đầu tiến trình của chúng ở trong RAM, khiến Kaspersky Endpoint Security không thể loại trừ chúng bằng các phương thức khác. Kết quả là mối đe dọa này sẽ được vô hiệu hóa. Trong khi quá trình Khử nhiễm Cao cấp đang diễn ra, bạn được khuyến nghị hạn chế bắt đầu các tiến trình mới hoặc sửa registry hệ điều hành. Công nghệ khử nhiễm cao cấp này sử dụng lượng tài nguyên hệ điều hành đáng kể và có thể làm chậm các ứng dụng khác.

Sau khi quá trình Khử nhiễm Cao cấp đã được hoàn tất trên một máy tính chạy Microsoft Windows cho máy trạm, Kaspersky Endpoint Security sẽ yêu cầu người dùng khởi động lại máy tính. Sau khi hệ thống được khởi động lại, Kaspersky Endpoint Security sẽ xóa các tập tin phần mềm độc hại và bắt đầu một tác vụ quét đầy đủ "nhẹ" trên toàn máy tính.

Không thể nhắc khởi động lại trên một máy tính chạy Microsoft Windows cho máy chủ tập tin, bởi các đặc trưng của Kaspersky Endpoint Security cho máy chủ tập tin. Một tác vụ khởi động lại máy chủ tập tin không theo kế hoạch có thể dẫn đến các vấn đề liên quan đến việc dữ liệu máy chủ tập tin tạm thời không khả dụng, hoặc mất dữ liệu chưa được lưu lại. Bạn được khuyến nghị chỉ khởi động lại một máy chủ tập tin theo lịch trình. Đó là lý do công nghệ Khử nhiễm Cao cấp bị tắt cho máy chủ tập tin ở chế độ mặc định.

Nếu tình trạng lây nhiễm bị phát hiện trên một máy chủ tập tin, một sự kiện sẽ được chuyển đến Kaspersky Security Center với thông tin rằng cần Khử nhiễm Chủ động. Để khử nhiễm một tình trạng lây nhiễm trên máy chủ tập tin, hãy bật công nghệ Khử nhiễm Chủ động cho máy chủ tập tin và bắt đầu một tác vụ nhóm *Quét virus* tại thời điểm thuận lợi cho những người dùng máy chủ tập tin.

Chọn các loại đối tượng có thể được phát hiện

Để chọn các loại đối tượng có thể được phát hiện:

1. Mở cửa sổ cấu hình ứng dụng.
2. Ở phần bên trái của cửa sổ, chọn mục **Bảo vệ Chống virus**.
   Cấu hình bảo vệ chống virus sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Trong mục **Đối tượng**, nhấn nút **Cấu hình**.
   Cửa sổ **Phát hiện đối tượng** sẽ được mở ra.
4. Chọn hộp kiểm đối diện các loại đối tượng mà bạn muốn Kaspersky Endpoint Security phát hiện:
   - **Công cụ độc hại**
   - **Phần mềm quảng cáo**
   - **Tự động quay số**
   - **Khác**
   - **Các tập tin đóng gói có thể gây nguy hiểm**
   - **Các tập tin nén**

5. Nhấn **OK**.

   Cửa sổ **Phát hiện đối tượng** sẽ được đóng lại. Trong mục **Đối tượng**, các loại đối tượng được chọn sẽ được liệt kê trong phần **Đang bật tính năng phát hiện các kiểu đối tượng sau**.

6. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Bật hoặc tắt công nghệ Khử nhiễm Cao cấp cho máy trạm

Để bật hoặc tắt công nghệ Khử nhiễm Cao cấp cho máy trạm:

1. Mở cửa sổ cấu hình ứng dụng.
2. Ở phần bên trái của cửa sổ, chọn mục **Bảo vệ Chống virus**.

   Cấu hình bảo vệ chống virus sẽ được hiển thị ở phần bên phải của cửa sổ.

3. Trong phần bên phải của cửa sổ, thực hiện một trong các thao tác sau:

   - Chọn **Cho phép Công nghệ khử mã độc nâng cao** để bật công nghệ khử nhiễm cao cấp.
   - Xóa **Cho phép Công nghệ khử mã độc nâng cao** để tắt công nghệ khử nhiễm cao cấp.

4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Khi tác vụ Khử nhiễm Cao cấp được bắt đầu thông qua Kaspersky Security Center, phần lớn các chức năng của hệ điều hành sẽ tạm thời không khả dụng đối với người dùng. Máy trạm sẽ được khởi động lại sau khi tác vụ đã hoàn tất.

Bật hoặc tắt công nghệ Khử nhiễm Cao cấp cho máy chủ tập tin

Để bật công nghệ Khử nhiễm Cao cấp cho máy chủ tập tin, thực hiện một trong các hành động sau:

- Bật công nghệ Khử nhiễm Cao cấp trong thuộc tính của chính sách Kaspersky Security Center đang có hiệu lực. Để làm điều này:

  a. Mở mục **Cấu hình bảo vệ tổng quát** trong cửa sổ thuộc tính chính sách.

  b. Chọn hộp kiểm **Cho phép Công nghệ khử mã độc nâng cao**.

  c. Để lưu lại thay đổi, chọn **OK** trong cửa sổ thuộc tính chính sách.

- Trong thuộc tính của tác vụ nhóm Quét virus của Kaspersky Security Center, chọn hộp kiểm **Chạy khử mã độc nâng cao ngay lập tức**.

Để tắt công nghệ Khử nhiễm Cao cấp cho máy chủ tập tin, thực hiện một trong các hành động sau:

- Tắt công nghệ Khử nhiễm Cao cấp trong thuộc tính của chính sách Kaspersky Security Center. Để làm điều này:

  a. Mở mục **Cấu hình bảo vệ tổng quát** trong cửa sổ thuộc tính chính sách.

b. Xóa hộp kiểm **Cho phép Công nghệ khử mã độc nâng cao**.

c. Để lưu lại thay đổi, chọn **OK** trong cửa sổ thuộc tính chính sách.

- Trong thuộc tính của tác vụ nhóm Quét virus của Kaspersky Security Center, xóa hộp kiểm **Chạy khử mã độc nâng cao ngay lập tức**.

Bật hoặc tắt chế độ tiết kiệm năng lượng

Để bật hoặc tắt chế độ tiết kiệm năng lượng:

1. Mở cửa sổ cấu hình ứng dụng.
2. Ở phần bên trái của cửa sổ, chọn mục **Cấu hình nâng cao**.
   Cấu hình nâng cao của ứng dụng sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Trong mục **Chế độ hoạt động**, nhấn nút **Cấu hình**.
   Cửa sổ **Chế độ hoạt động** sẽ được mở ra.
4. Thực thi các hành động sau trong cửa sổ **Chế độ hoạt động**:
   - Để bật chế độ tiết kiệm năng lượng, chọn hộp kiểm **Hoãn các tác vụ đã lập lịch khi đang sử dụng pin**.
     Khi chế độ tiết kiệm năng lượng đang được bật và máy tính đang chạy pin, các tác vụ sau đây sẽ không được chạy kể cả khi đã được xếp lịch:
     - Tác vụ cập nhật
     - Tác vụ Quét Toàn bộ
     - Tác vụ Quét khu vực quan trọng
     - Tác vụ Quét Tùy chỉnh
     - Tác vụ Quét lỗ hổng bảo mật
     - Tác vụ Kiểm tra Tính Toàn vẹn
   - Nếu bạn muốn tắt chế độ tiết kiệm năng lượng, xóa hộp kiểm **Hoãn các tác vụ đã lập lịch khi đang sử dụng pin**. Trong trường hợp này, Kaspersky Endpoint Security sẽ thực thi các tác vụ đã được lập lịch bất kể nguồn năng lượng của máy tính là gì.
5. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Bật hoặc tắt tính năng nhường tài nguyên cho các ứng dụng khác

Để bật hoặc tắt tính năng nhường tài nguyên cho các ứng dụng khác:

1. Mở cửa sổ cấu hình ứng dụng.

2. Ở phần bên trái của cửa sổ, chọn mục **Cấu hình nâng cao**.

   Cấu hình nâng cao của ứng dụng sẽ được hiển thị ở phần bên phải của cửa sổ.

3. Trong mục **Chế độ hoạt động**, nhấn nút **Cấu hình**.

   Cửa sổ **Chế độ hoạt động** sẽ được mở ra.

4. Thực thi các hành động sau trong cửa sổ **Chế độ hoạt động**:

   - Nếu bạn muốn bật chế độ trong đó các tài nguyên được nhường cho các ứng dụng khác, chọn hộp kiểm **Nhường tài nguyên cho các ứng dụng khác**.

     Khi được thiết lập để nhường tài nguyên cho các ứng dụng khác, Kaspersky Endpoint Security sẽ hoãn các tác vụ được lập lịch có thể làm chậm các ứng dụng khác:

     - Tác vụ cập nhật
     - Tác vụ Quét Toàn bộ
     - Tác vụ Quét khu vực quan trọng
     - Tác vụ Quét Tùy chỉnh
     - Tác vụ Quét lỗ hổng bảo mật
     - Tác vụ Kiểm tra Tính Toàn vẹn

   - Nếu bạn muốn tắt chế độ trong đó các tài nguyên được nhường cho các ứng dụng khác, xóa hộp kiểm **Nhường tài nguyên cho các ứng dụng khác**. Trong trường hợp này, Kaspersky Endpoint Security sẽ thực thi các tác vụ đã được lập lịch bất kể hoạt động của các ứng dụng khác.

   Theo mặc định, ứng dụng được thiết lập để nhường tài nguyên cho các ứng dụng khác.

5. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Mật khẩu bảo vệ

Phần này chứa thông tin về hạn chế truy cập đến Kaspersky Endpoint Security với một mật khẩu.

Thông tin về hạn chế truy cập đến Kaspersky Endpoint Security

Nhiều người dùng với các cấp độ thông thạo máy tính khác nhau có thể dùng chung một máy tính. Nếu nhiều người dùng đều có truy cập không hạn chế đến Kaspersky Endpoint Security cùng các cấu hình của ứng dụng, cấp độ bảo vệ máy tính tổng quát có thể bị ảnh hưởng.

Bạn có thể hạn chế truy cập đến Kaspersky Endpoint Security bằng cách thiết lập một tên người dùng và mật khẩu và quy định các hoạt động mà ở đó ứng dụng sẽ nhắc người dùng nhập những chứng chỉ này:

Khi một phiên bản cũ của ứng dụng được nâng cấp lên Kaspersky Endpoint Security 10 Service Pack 2 for Windows, mật khẩu vẫn sẽ được giữ nguyên (nếu nó đã được đặt). Để sửa cấu hình mật khẩu bảo vệ ở lần đầu tiên, hãy sử dụng tên người dùng KLAdmin mặc định.

Bật và tắt bảo vệ bằng mật khẩu

Chúng tôi khuyến nghị bạn nên cẩn thận khi sử dụng mật khẩu để hạn chế truy cập đến ứng dụng. Nếu bạn quên mật khẩu, hãy liên hệ với Hỗ trợ kỹ thuật của Kaspersky để được chỉ dẫn cách tắt mật khẩu bảo vệ.

Để bật bảo vệ bằng mật khẩu:

1. Mở cửa sổ cấu hình ứng dụng.
2. Ở phần bên trái của cửa sổ, chọn mục **Cấu hình nâng cao**.

   Cấu hình của ứng dụng sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Trong mục **Mật khẩu bảo vệ**, nhấn nút **Cấu hình**.

   Cửa sổ **Mật khẩu bảo vệ** sẽ được mở ra.
4. Chọn hộp kiểm **Cho phép mật khẩu bảo vệ**.
5. Trong trường **Tên người dùng**, nhập tên người dùng được yêu cầu trong cửa sổ **Kiểm tra mật khẩu** khi thực hiện các thao tác bảo vệ mật khẩu sau đó.
6. Trong trường **Mật khẩu mới**, nhập một mật khẩu để truy cập ứng dụng.
7. Xác nhận mật khẩu trong trường **Xác nhận mật khẩu**.
8. Nếu bạn muốn hạn chế truy cập cho tất cả các hoạt động của ứng dụng, trong mục **Phạm vi mật khẩu**, nhấn nút **Chọn tất cả**.
9. Nếu bạn muốn hạn chế truy cập người dùng một cách chọn lọc, trong mục **Phạm vi mật khẩu**, chọn các hộp kiểm cạnh tên của các hoạt động liên quan:
   - **Thiết lập cấu hình ứng dụng**.
   - **Thoát khỏi ứng dụng**.
   - **Tắt các thành phần bảo vệ**.
   - **Vô hiệu các thành phần kiểm soát**.
   - **Xóa key**.
   - **Gỡ bỏ / thay đổi / khôi phục ứng dụng**.
   - **Khôi phục quyền truy cập vào dữ liệu trên ổ đĩa mã hóa**.
   - **Xem báo cáo**.
10. Nhấn nút **OK**.

    Ứng dụng sẽ xác thực mật khẩu được nhập. Nếu mật khẩu khớp nhau, ứng dụng sẽ áp dụng mật khẩu. Nếu mật khẩu không khớp, ứng dụng sẽ nhắc bạn xác nhận mật khẩu một lần nữa trong trường **Xác nhận mật khẩu**.

Sau khi bảo vệ mật khẩu được bật, ứng dụng sẽ hỏi mật khẩu mỗi lần một thao tác được bao gồm trong phạm vi mật khẩu được thực hiện. Nếu bạn không muốn ứng dụng nhắc bạn nhập mật khẩu mỗi khi bạn thực hiện một hoạt động được bảo vệ bởi mật khẩu trong phiên làm việc hiện tại, bạn có thể chọn hộp kiểm **Lưu mật khẩu cho phiên làm việc hiện hành** trong cửa sổ **Kiểm tra mật khẩu**.

Khi hộp kiểm **Lưu mật khẩu cho phiên làm việc hiện hành** bị xóa, ứng dụng sẽ nhắc bạn nhập mật khẩu mỗi lần bạn cố gắng thực hiện hoạt động có mật khẩu bảo vệ.

Để tắt mật khẩu bảo vệ:

1. Mở cửa sổ cấu hình ứng dụng.
2. Ở phần bên trái của cửa sổ, chọn mục **Cấu hình nâng cao**.
   Cấu hình của ứng dụng sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Trong mục **Mật khẩu bảo vệ**, nhấn nút **Cấu hình**.
   Cửa sổ **Mật khẩu bảo vệ** sẽ được mở ra.
4. Xóa hộp kiểm **Cho phép mật khẩu bảo vệ**.

   Bạn chỉ có thể tắt Bảo vệ bằng mật khẩu nếu bạn đăng nhập là KLAdmin. Bạn không thể tắt bảo vệ bằng mật khẩu nếu bạn đang sử dụng một tài khoản người dùng khác hoặc một mật khẩu tạm thời.

5. Nhấn nút **OK**.

Sau khi bảo vệ mật khẩu bị tắt, việc hạn chế truy cập đến ứng dụng sẽ bị hủy bỏ ở lần khởi động tiếp theo của Kaspersky Endpoint Security.

Sửa mật khẩu truy cập Kaspersky Endpoint Security

Để thay đổi mật khẩu truy cập Kaspersky Endpoint Security:

1. Mở cửa sổ cấu hình ứng dụng.
2. Ở phần bên trái của cửa sổ, chọn mục **Cấu hình nâng cao**.
3. Trong mục **Mật khẩu bảo vệ**, nhấn nút **Cấu hình**.
   Cửa sổ **Mật khẩu bảo vệ** sẽ được mở ra.
4. Nhập tên người dùng vào trường **Tên người dùng**.
5. Trong trường **Mật khẩu mới**, nhập một mật khẩu mới để truy cập ứng dụng.
6. Trong trường **Xác nhận mật khẩu**, nhập mật khẩu mới một lần nữa.
7. Nhấn **OK**.
   Ứng dụng sẽ xác thực mật khẩu được nhập. Nếu mật khẩu khớp nhau, ứng dụng sẽ áp dụng mật khẩu mới và đóng cửa sổ **Mật khẩu bảo vệ**. Nếu mật khẩu không khớp, ứng dụng sẽ nhắc bạn xác nhận mật khẩu một lần nữa trong trường **Xác nhận mật khẩu**.

8. Để lưu lại các thay đổi, trong cửa sổ cấu hình ứng dụng, nhấn nút **Lưu**.

Thông tin về việc sử dụng một mật khẩu tạm thời

Khi làm việc trên các máy khách được quản lý bởi một chính sách Kaspersky Security Center, người dùng có thể sẽ cần thực hiện các hoạt động với Kaspersky Endpoint Security được bảo vệ bởi mật khẩu ở cấp độ chính sách. Khi mật khẩu bảo vệ được bật, chỉ quản trị viên Kaspersky Security Center mới có thể thực hiện hoạt động được quy định trong phạm vi mật khẩu. Tuy nhiên, nếu kết nối với Kaspersky Security Center đã bị mất (ví dụ như khi người dùng ở ngoài mạng doanh nghiệp), các chức năng để làm việc với giao diện cục bộ của Kaspersky Security Center sẽ bị giới hạn.

Để cho phép người dùng thực hiện các hoạt động cần thiết mà không cung cấp cho họ mật khẩu được đặt trong cấu hình chính sách, quản trị viên Kaspersky Security Center có thể tạo một mật khẩu tạm thời. Một mật khẩu tạm thời có thời hạn hiệu lực giới hạn và phạm vi hành động giới hạn. Sau khi người dùng nhập mật khẩu tạm thời vào giao diện cục bộ của ứng dụng, các hoạt động được cho phép bởi quản trị viên Kaspersky Security Center sẽ có thể được thực hiện.

Khi mật khẩu tạm thời hết hạn, Kaspersky Endpoint Security sẽ tiếp tục vận hành theo cấu hình của chính sách Kaspersky Security Center. Các hoạt động được bảo vệ bởi mật khẩu ở cấp độ chính sách sẽ không thể được thực hiện bởi người dùng.

Tạo một mật khẩu tạm thời sử dụng Bảng điều khiển Quản trị của Kaspersky Security Center

Để tạo một mật khẩu tạm thời và gửi nó đến người dùng:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.

2. Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, mở thư mục với tên của nhóm quản trị chứa máy tính của người dùng yêu cầu mật khẩu tạm thời.

3. Trong không gian làm việc, chọn thẻ **Các thiết bị**.

4. Trong menu ngữ cảnh của máy tính của người dùng yêu cầu mật khẩu tạm thời, chọn **Thuộc tính**.
   Cửa sổ **Thuộc tính:: <Tên máy tính>** sẽ được mở ra.

5. Trong cửa sổ **Thuộc tính: <Tên máy tính>**, chọn mục **Ứng dụng**.

6. Chọn Kaspersky Endpoint Security Service Pack 2 for Windows và mở cửa sổ thuộc tính ứng dụng bằng một trong các phương thức sau đây:

   - Nhấn nút **Thuộc tính** ở dưới màn hình.
   - Trong menu ngữ cảnh của ứng dụng, chọn **Thuộc tính**.

   Việc này sẽ mở ra cửa sổ **Cấu hình của ứng dụng "<Tên ứng dụng>"**.

7. Trong cửa sổ **Cấu hình của ứng dụng "<Tên ứng dụng>"**, trong mục **Cấu hình nâng cao**, chọn mục con **Cấu hình ứng dụng**.

8. Trong mục **Mật khẩu bảo vệ**, nhấn nút **Cấu hình**.

Cửa sổ **Mật khẩu bảo vệ** sẽ được mở ra.

9. Trong cửa sổ **Mật khẩu bảo vệ**, trong mục **Mật khẩu tạm thời**, nhấn nút **Cấu hình**.

   Nút này có thể được sử dụng nếu mật khẩu bảo vệ được bật cho Kaspersky Security Center trong chính sách Kaspersky Security Center được chạy trên máy tính.

   Cửa sổ **Tạo mật khẩu tạm thời** sẽ được mở ra.

10. Trong trường **Ngày hết hạn**, quy định ngày mà người dùng sẽ không thể sử dụng mật khẩu tạm thời nữa.

    Vào ngày này, mật khẩu tạm thời sẽ trở nên vô hiệu. Một mật khẩu tạm thời mới phải được tạo để cấp quyền truy cập và thực hiện các hoạt động trong giao diện cục bộ của Kaspersky Endpoint Security.

11. Trong bảng **Phạm vi mật khẩu tạm thời**, chọn hộp kiểm đối diện các hoạt động có thể được thực thi bởi người dùng khi mật khẩu tạm thời còn hiệu lực.

12. Nhấn nút **Tạo**.

    Việc này sẽ mở ra cửa sổ **Mật khẩu tạm thời** chứa một mật khẩu được mã hóa.

13. Sao chép mật khẩu đó cùng hướng dẫn cách áp dụng mật khẩu và gửi chúng đến người dùng.

Áp dụng một mật khẩu tạm thời trong giao diện Kaspersky Endpoint Security

Các chỉ dẫn này dành cho người sử dụng của máy khách có cài đặt Kaspersky Endpoint Security.

Để áp dụng một mật khẩu tạm thời:

1. Mở cửa sổ cấu hình ứng dụng.
2. Ở phần bên trái của cửa sổ, chọn mục **Cấu hình nâng cao**.

   Cấu hình của ứng dụng sẽ được hiển thị ở phần bên phải của cửa sổ.

3. Trong mục **Mật khẩu bảo vệ**, nhấn nút **Mật khẩu tạm thời**.

   Cửa sổ **Mật khẩu tạm thời** sẽ được mở ra.

4. Chọn hộp kiểm **Bật mật khẩu tạm thời**.
5. Trong trường nhập liệu, nhập mật khẩu được nhận từ quản trị viên Kaspersky Security Center.
6. Nhấn **OK** để lưu lại các thay đổi.

Sau khi mật khẩu tạm thời đã được áp dụng, các hoạt động được quy định bởi quản trị viên Kaspersky Security Center sẽ có thể được thực hiện. Cửa sổ **Mật khẩu tạm thời** sẽ hiển thị ngày hết hạn của mật khẩu tạm thời và các hoạt động được cho phép.

Quản trị ứng dụng từ xa thông qua Kaspersky Security Center

Phần này mô tả tính năng quản trị từ xa Kaspersky Endpoint Security thông qua Kaspersky Security Center.

Thông tin về quản lý ứng dụng thông qua Kaspersky Security Center

Kaspersky Security Center cho phép bạn cài đặt và gỡ bỏ, khởi động và dừng Kaspersky Endpoint Security từ xa, cũng như thiết lập cấu hình ứng dụng, thay đổi các nhóm thành phần ứng dụng có thể được sử dụng, bổ sung khóa, và bắt đầu các tác vụ cập nhật và quét.

Để biết thêm thông tin về việc quản lý ứng dụng thông qua Kaspersky Security Center không được cung cấp trong tài liệu này, vui lòng tham khảo *Hướng dẫn dành cho Quản trị viên Kaspersky Security Center*.

Ứng dụng có thể được quản lý qua Kaspersky Security Center sử dụng tiện ích quản trị Kaspersky Endpoint Security.

Phiên bản của tiện ích quản trị có thể khác với phiên bản Kaspersky Endpoint Security được cài đặt trên máy khách. Nếu phiên bản được cài đặt của tiện ích quản trị có ít chức năng hơn phiên bản được cài đặt của Kaspersky Endpoint Security, cấu hình của những chức năng bị thiếu sẽ không được quản lý bởi tiện ích quản trị. Các cấu hình này có thể được sửa đổi bởi người dùng trong giao diện cục bộ của Kaspersky Endpoint Security.

Các cân nhắc đặc biệt khi làm việc với các phiên bản khác nhau của tiện ích quản trị

Bạn có thể sử dụng một tiện ích quản trị để thay đổi các đề mục sau:

- Chính sách
- Hồ sơ chính sách
- Tác vụ nhóm
- Tác vụ cục bộ
- Cấu hình cục bộ của Kaspersky Endpoint Security

Bạn chỉ có thể quản lý Kaspersky Endpoint Security qua Kaspersky Security Center nếu bạn có một tiện ích quản trị với phiên bản bằng hoặc mới hơn phiên bản được quy định trong thông tin liên quan đến tính tương thích của Kaspersky Endpoint Security với tiện ích quản trị. Bạn có thể xem phiên bản tối thiểu được yêu cầu của tiện ích quản trị trong tập tin installer.ini trong gói phân phối.

Nếu có bất kỳ thành phần nào được mở, tiện ích quản trị sẽ kiểm tra thông tin tương thích của nó. Nếu phiên bản của tiện ích quản trị bằng hoặc mới hơn phiên bản được quy định trong thông tin tương thích, bạn có thể thay đổi cấu hình của thành phần này. Nếu không, bạn không thể sử dụng tiện ích quản trị để thay đổi các cấu hình của thành phần được chọn. Bạn được khuyến nghị nâng cấp tiện ích quản trị.

Thay đổi các cấu hình được quy định từ trước sử dụng một phiên bản mới hơn của tiện ích quản trị.

Bạn có thể sử dụng một phiên bản mới hơn của tiện ích quản trị để thay đổi tất cả các cấu hình đã được quy định từ trước, và thiết lập các cấu hình mới không có trong phiên bản trước đó của tiện ích quản trị.

Đối với các cấu hình mới, một phiên bản mới hơn của tiện ích quản trị sẽ gán các giá trị mặc định khi một chính sách, hồ sơ chính sách hoặc tác vụ lần đầu tiên được lưu.

Sau khi bạn đã thay đổi cấu hình của một chính sách, hồ sơ chính sách hoặc tác vụ nhóm sử dụng một phiên bản mới hơn của tiện ích quản trị, các thành phần này sẽ trở nên không khả dụng đối với phiên bản trước đó của tiện ích quản trị. Cấu hình cục bộ của Kaspersky Endpoint Security cùng cấu hình của các tác vụ cục bộ sẽ vẫn có thể được sử dụng cho tiện ích quản trị của các phiên bản trước.

Bắt đầu và dừng Kaspersky Endpoint Security trên một máy khách

Để bắt đầu hoặc dừng một ứng dụng trên một máy khách:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, mở thư mục với tên của nhóm quản trị chứa máy khách liên quan.
3. Trong không gian làm việc, chọn thẻ **Các thiết bị**.
4. Chọn máy tính mà trên đó bạn muốn bắt đầu hoặc dừng ứng dụng.
5. Phải chuột để hiển thị menu ngữ cảnh của máy khách và chọn **Thuộc tính**.

   Một cửa sổ thuộc tính máy khách sẽ được mở ra.
6. Trong cửa sổ thuộc tính máy khách, chọn phần **Ứng dụng**.

   Một danh sách các ứng dụng Kaspersky được cài đặt trên máy khách sẽ được hiển thị ở phần bên phải của cửa sổ thuộc tính máy khách.
7. Chọn Kaspersky Endpoint Security 10 for Windows
8. Làm các bước sau:

   - Để bắt đầu ứng dụng, nhấn nút ở bên phải danh sách các ứng dụng Kaspersky hoặc thực hiện hành động sau:

     a. Chọn **Thuộc tính** trong menu ngữ cảnh của Kaspersky Endpoint Security hoặc nhấn nút **Thuộc tính** ở dưới danh sách các ứng dụng Kaspersky.

     Cửa sổ **Cấu hình ứng dụng Kaspersky Endpoint Security 10 for Windows** sẽ được mở ra.

     b. Trong mục **Tổng quát**, nhấn nút **Chạy** ở bên phải của cửa sổ.

   - Để dừng ứng dụng, nhấn nút ở bên phải danh sách các ứng dụng Kaspersky hoặc thực hiện hành động sau:

     a. Chọn **Thuộc tính** trong menu ngữ cảnh của Kaspersky Endpoint Security hoặc nhấn nút **Thuộc tính** ở dưới danh sách các ứng dụng Kaspersky.

     Cửa sổ **Cấu hình ứng dụng Kaspersky Endpoint Security 10 for Windows** sẽ được mở ra.

b. Trong mục **Tổng quát**, nhấn nút **Dừng** ở bên phải của cửa sổ.

Thiết lập cấu hình Kaspersky Endpoint Security

Để thiết lập cấu hình Kaspersky Endpoint Security:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, mở thư mục với tên của nhóm quản trị chứa máy khách liên quan.
3. Trong không gian làm việc, chọn thẻ **Các thiết bị**.
4. Chọn máy tính mà bạn muốn thiết lập cấu hình Kaspersky Endpoint Security.
5. Trong menu ngữ cảnh của máy khách, chọn **Thuộc tính**.

   Một cửa sổ thuộc tính máy khách sẽ được mở ra.
6. Trong cửa sổ thuộc tính máy khách, chọn phần **Ứng dụng**.

   Một danh sách các ứng dụng Kaspersky được cài đặt trên máy khách sẽ được hiển thị ở phần bên phải của cửa sổ thuộc tính máy khách.
7. Chọn ứng dụng Kaspersky Endpoint Security 10 for Windows.
8. Thực hiện một trong các thao tác sau:

   - Chọn **Thuộc tính** từ menu ngữ cảnh của Kaspersky Endpoint Security 10 for Windows.
   - Nhấn nút **Thuộc tính** ở dưới danh sách các ứng dụng Kaspersky.

   Cửa sổ **Cấu hình ứng dụng Kaspersky Endpoint Security 10 for Windows** sẽ được mở ra.
9. Trong mục **Cấu hình nâng cao**, thiết lập cấu hình cho Kaspersky Endpoint Security cũng như các cấu hình báo cáo và lưu trữ.

   Các mục khác của cửa sổ **Cấu hình ứng dụng Kaspersky Endpoint Security 10 for Windows** cũng giống như các mục ứng dụng tiêu chuẩn của Kaspersky Security Center. Một mô tả về những mục này cũng được cung cấp trong *Hướng dẫn dành cho Quản trị viên Kaspersky Security Center*.

   > Nếu một ứng dụng phải tuân thủ một chính sách cấm các thay đổi đến những cấu hình cụ thể, bạn sẽ không thể sửa chúng trong khi thiết lập cấu hình ứng dụng trong mục **Cấu hình nâng cao**.
10. Để lưu lại các thay đổi, trong cửa sổ **Cấu hình ứng dụng Kaspersky Endpoint Security 10 for Windows**, nhấn nút **OK**.

Quản lý các tác vụ

Phần này mô tả cách quản lý tác vụ cho Kaspersky Endpoint Security. Xem *Hướng dẫn dành cho Quản trị viên Kaspersky Security Center* để biết chi tiết về việc quản lý tác vụ thông qua Kaspersky Security Center.

Thông tin về các tác vụ cho Kaspersky Endpoint Security

Kaspersky Security Center kiểm soát hoạt động của các ứng dụng Kaspersky trên các máy khách thông qua các tác vụ. Các tác vụ thực thi những chức năng quản trị chính, ví dụ như cài đặt khóa, quét máy tính, cũng như cập nhật cơ sở dữ liệu và mô-đun phần mềm ứng dụng.

Bạn có thể tạo các loại tác vụ sau để quản trị Kaspersky Endpoint Security thông qua Kaspersky Security Center:

- Các tác vụ cục bộ được thiết lập cho một máy khách riêng lẻ.
- Các tác vụ nhóm được thiết lập cho các máy khách trong các nhóm quản trị.
- Các tác vụ cho một nhóm máy tính không thuộc nhóm quản trị.

  Các tác vụ cho các nhóm máy tính nằm ngoài nhóm quản trị chỉ áp dụng cho các máy khách được quy định trong cấu hình tác vụ. Nếu các máy khách mới được bổ sung vào nhóm máy tính được thiết lập một tác vụ, tác vụ này sẽ không được áp dụng cho các máy tính mới này. Để áp dụng tác vụ đến các máy tính này, hãy tạo một tác vụ mới hoặc sửa cấu hình của tác vụ sẵn có.

Để quản lý từ xa Kaspersky Endpoint Security, bạn có thể sử dụng các tác vụ sau thuộc mọi thể loại được liệt kê:

- **Thêm key**. Kaspersky Endpoint Security sẽ thêm một khóa để kích hoạt ứng dụng, bao gồm một khóa bổ sung.
- **Thay đổi thành phần ứng dụng**. Kaspersky Endpoint Security sẽ cài đặt hoặc gỡ bỏ các thành phần trên máy khách theo danh sách các thành phần được quy định trong cấu hình tác vụ.
- **Kho**. Kaspersky Endpoint Security sẽ thu thập thông tin về tất cả các tập tin thực thi của ứng dụng được lưu trữ trên máy tính.

  Bạn có thể bật tính năng lưu kho mô-đun DLL và các tập tin kịch bản. Trong trường hợp này, Kaspersky Security Center sẽ nhận thông tin về các mô-đun DLL được nạp trên máy tính có cài đặt Kaspersky Endpoint Security, và về các tập tin chứa kịch bản.

  Việc lưu kho mô-đun DLL và các tập tin kịch bản sẽ làm tăng đáng kể thời gian tác vụ lưu kho và kích cỡ cơ sở dữ liệu.

- **Cập nhật**. Kaspersky Endpoint Security sẽ cập nhật cơ sở dữ liệu và mô-đun ứng dụng theo cấu hình cập nhật đã được thiết lập.
- **Khôi phục**. Kaspersky Endpoint Security sẽ khôi phục lại bản cập nhật cơ sở dữ liệu và mô-đun gần nhất.
- **Quét virus**. Kaspersky Endpoint Security sẽ quét các khu vực máy tính được quy định trong cấu hình tác vụ để phát hiện virus và các mối đe dọa khác.

- **Kiểm tra kết nối với KSN**. Kaspersky Endpoint Security sẽ gửi một truy vấn về tình trạng khả dụng của các máy chủ KSN và cập nhật trạng thái kết nối với KSN.
- **Kiểm tra Tính Toàn vẹn**. Kaspersky Endpoint Security sẽ nhận dữ liệu về các nhóm mô-đun ứng dụng được cài đặt trên máy khách và quét chữ ký điện tử của từng mô-đun.
- **Quản lý tài khoản Authentication Agent**. Khi thực hiện tác vụ này, Kaspersky Endpoint Security sẽ tạo các lệnh để xóa, thêm hoặc thay đổi các tài khoản Authentication Agent.

Bạn có thể thực hiện các hành động sau với các tác vụ:

- Bắt đầu, dừng, tạm ngưng và khôi phục các tác vụ.
- Tạo tác vụ mới.
- Sửa cấu hình tác vụ.

Quyền truy cập đến cấu hình của các tác vụ Kaspersky Endpoint Security (đọc, ghi, thực thi) được quy định cho mỗi người dùng có thể truy cập Máy chủ Quản trị của Kaspersky Security Center, thông qua việc cấu hình quyền truy cập đến các khu vực chức năng của Kaspersky Endpoint Security. Để thiết lập truy cập đến các khu vực chức năng của Kaspersky Endpoint Security, truy cập mục **Bảo mật** của cửa sổ thuộc tính của Máy chủ Quản trị của Kaspersky Security Center.

Thiết lập chế độ quản lý tác vụ

Để thiết lập chế độ làm việc với các tác vụ trong giao diện cục bộ của Kaspersky Endpoint Security:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, mở thư mục với tên của nhóm quản trị mà bạn muốn thiết lập chế độ làm việc với các tác vụ trong giao diện cục bộ của Kaspersky Endpoint Security.
3. Trong không gian làm việc, chọn thẻ **Chính sách**.
4. Chọn chính sách cần thiết.
5. Mở cửa sổ **Thuộc tính: <Tên chính sách>** sử dụng một trong những phương pháp sau đây:
   - Trong menu ngữ cảnh của chính sách, chọn **Thuộc tính**.
   - Nhấn vào liên kết **Thiết lập chính sách** được đặt ở phần bên phải của không gian làm việc của Bảng điều khiển Quản trị.
6. Trong mục **Cấu hình nâng cao**, chọn mục con **Cấu hình ứng dụng**.
7. Trong mục **Chế độ hoạt động**:
   - Nếu bạn muốn cho phép người dùng làm việc với các tác vụ cục bộ trong giao diện và dòng lệnh của Kaspersky Endpoint Security, chọn hộp kiểm **Cho phép sử dụng tác vụ nội bộ**.

     Nếu hộp kiểm bị xóa, chức năng của các tác vụ cục bộ sẽ bị dừng. Trong chế độ này, các tác vụ cục bộ sẽ không chạy theo lịch. Các tác vụ cục bộ cũng sẽ không thể được bắt đầu và sửa trong giao diện cục bộ của Kaspersky Endpoint Security, và khi làm việc với dòng lệnh.

- Nếu bạn muốn cho phép người dùng xem danh sách các tác vụ nhóm, chọn hộp kiểm **Cho phép các tác vụ nhóm được hiển thị**.
- Nếu bạn muốn cho phép người dùng sửa cấu hình của các tác vụ nhóm, chọn hộp kiểm **Cho phép quản lý tác vụ của nhóm**.

8. Nhấn **OK** để lưu thay đổi.
9. Áp dụng chính sách.

   Xem *Hướng dẫn dành cho Quản trị viên Kaspersky Security Center* để biết chi tiết về việc áp dụng các chính sách Kaspersky Security Center.

Tạo một tác vụ cục bộ

Để tạo một tác vụ cục bộ:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, mở thư mục với tên của nhóm quản trị chứa máy khách liên quan.
3. Trong không gian làm việc, chọn thẻ **Các thiết bị**.
4. Chọn máy tính mà bạn muốn tạo một tác vụ cục bộ.
5. Thực hiện một trong các thao tác sau:
   - Trong menu ngữ cảnh của máy khách, chọn mục **Tất cả tác vụ** Tạo tác vụ.
   - Trong menu ngữ cảnh của máy khách, chọn **Thuộc tính**, và trong cửa sổ **Thuộc tính: <Tên máy tính>** được mở ra, trên thẻ **Tác vụ**, nhấn nút **Thêm**.
   - Trong danh sách thả xuống **Đề xuất xử lý**, chọn **Tạo tác vụ**.

   Trình hướng dẫn Tác vụ sẽ được bắt đầu.
6. Làm theo chỉ dẫn của Trình hướng dẫn Tác vụ.

Tạo một tác vụ nhóm

Để tạo một tác vụ nhóm:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Thực hiện một trong các thao tác sau:
   - Chọn thư mục **Quản lý thiết bị** trong cây Bảng điều khiển Quản trị để tạo một tác vụ nhóm cho tất cả các máy tính được quản lý bởi Kaspersky Security Center.
   - Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, chọn thư mục với tên của nhóm quản trị chứa máy khách liên quan.

3. Chọn thẻ **Tác vụ** trong không gian làm việc.
4. Nhấn nút **Tạo tác vụ**.
   Trình hướng dẫn Tác vụ sẽ được bắt đầu.
5. Làm theo chỉ dẫn của Trình hướng dẫn Tác vụ.

Tạo một tác vụ để lựa chọn thiết bị

Để tạo một tác vụ cho việc lựa chọn thiết bị, thực hiện các hành động sau:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Chọn thư mục **Tác vụ** trong cây Bảng điều khiển Quản trị.
3. Nhấn nút **Tạo tác vụ**.
   Trình hướng dẫn Tác vụ sẽ được bắt đầu.
4. Làm theo chỉ dẫn của Trình hướng dẫn Tác vụ.
5. Trong cửa sổ **Chọn thiết bị được gán tác vụ** của Trình hướng dẫn, nhấn nút **Gán tác vụ đến các thiết bị được chọn**.
6. Trong cửa sổ tiếp theo của Trình hướng dẫn, nhấn nút **Lựa chọn**.
   Cửa sổ **Chọn thiết bị** sẽ được mở ra.
7. Chọn các thiết bị cần thiết.
8. Nhấn nút **OK** trong cửa sổ **Chọn thiết bị**.
9. Làm theo chỉ dẫn của Trình hướng dẫn Tác vụ.

Bắt đầu, dừng, tạm ngưng và khôi phục một tác vụ

Nếu ứng dụng Kaspersky Endpoint Security đang chạy trên một máy khách, bạn có thể bắt đầu, dừng, tạm ngưng và khôi phục một tác vụ trên máy khách này thông qua Kaspersky Security Center. Khi Kaspersky Endpoint Security được tạm ngưng, việc chạy các tác vụ sẽ bị tạm ngưng và bạn không thể bắt đầu, dừng, tạm ngưng hay khôi phục một tác vụ thông qua Kaspersky Security Center.

Để bắt đầu, dừng, tạm ngưng hoặc khôi phục một tác vụ cục bộ:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, mở thư mục với tên của nhóm quản trị chứa máy khách liên quan.
3. Trong không gian làm việc, chọn thẻ **Các thiết bị**.

4. Chọn máy tính mà trên đó bạn muốn bắt đầu, dừng, tạm ngưng hoặc khôi phục một tác vụ cục bộ.

5. Phải chuột để hiển thị menu ngữ cảnh của máy khách và chọn **Thuộc tính**.

   Một cửa sổ thuộc tính máy khách sẽ được mở ra.

6. Lựa chọn mục **Tác vụ**.

   Một danh sách tác vụ cục bộ sẽ được hiển thị ở phần bên phải của cửa sổ.

7. Chọn một tác vụ cục bộ mà bạn muốn bắt đầu, dừng, tạm ngưng hoặc khôi phục.

8. Thực hiện hành động cần thiết trên tác vụ bằng cách sử dụng một trong các phương thức sau đây:

   - Nhấp chuột phải để mở menu ngữ cảnh của tác vụ cục bộ và chọn **Chạy** / **Dừng** / **Tạm ngưng** / **Khôi phục**.
   - Để bắt đầu hoặc dừng một tác vụ cục bộ, nhấn nút / ở phần bên phải của danh sách tác vụ cục bộ.
   - Làm các bước sau:

     a. Nhấn nút **Thuộc tính** ở dưới danh sách tác vụ cục bộ, hoặc chọn **Thuộc tính** trong menu ngữ cảnh tác vụ.

        Cửa sổ **Thuộc tính: <Tác vụ>** sẽ được mở ra.

     b. Trên thẻ **Tổng quát**, nhấn nút **Chạy** / **Dừng** / **Tạm ngưng** / **Khôi phục**.

Để bắt đầu, dừng, tạm ngưng hoặc khôi phục một tác vụ nhóm:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.

2. Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, mở thư mục với tên của nhóm quản trị mà bạn muốn bắt đầu, dừng, tạm ngưng hoặc khôi phục một tác vụ nhóm.

3. Chọn thẻ **Tác vụ** trong không gian làm việc.

   Các tác vụ nhóm sẽ được hiển thị ở phần bên phải của cửa sổ.

4. Chọn một tác vụ nhóm mà bạn muốn bắt đầu, dừng, tạm ngưng hoặc khôi phục.

5. Thực hiện hành động cần thiết trên tác vụ bằng cách sử dụng một trong các phương thức sau đây:

   - Trong menu ngữ cảnh của tác vụ nhóm, chọn **Chạy** / **Dừng** / **Tạm ngưng** / **Khôi phục**.
   - Nhấn vào nút / ở phần bên phải của cửa sổ để bắt đầu hoặc dừng một tác vụ nhóm.
   - Làm các bước sau:

     a. Nhấn vào liên kết **Cấu hình Tác vụ** ở phần bên phải không gian làm việc của Bảng điều khiển Quản trị, hoặc chọn **Thuộc tính** trong menu ngữ cảnh tác vụ.

        Cửa sổ **Thuộc tính: <Tác vụ>** sẽ được mở ra.

     b. Trên thẻ **Tổng quát**, nhấn nút **Chạy** / **Dừng** / **Tạm ngưng** / **Khôi phục**.

Để bắt đầu, dừng, tạm ngưng hoặc khôi phục một tác vụ cho một nhóm máy tính được lựa chọn:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Trong thư mục **Tác vụ** của cây Bảng điều khiển Quản trị, chọn tác vụ cho các máy tính được lựa chọn mà bạn muốn bắt đầu, dừng, tạm ngưng hoặc khôi phục.
3. Thực hiện một trong các thao tác sau:
   - Trong menu ngữ cảnh của tác vụ, chọn **Chạy** / **Dừng** / **Tạm ngưng** / **Khôi phục**.
   - Nhấn vào nút / ở phần bên phải của cửa sổ để bắt đầu hoặc dừng tác vụ cho các máy tính được quy định.
   - Làm các bước sau:
     a. Nhấn vào liên kết **Cấu hình Tác vụ** ở phần bên phải không gian làm việc của Bảng điều khiển Quản trị, hoặc chọn **Thuộc tính** trong menu ngữ cảnh tác vụ.
     Cửa sổ **Thuộc tính: <Tác vụ>** sẽ được mở ra.
     b. Trên thẻ **Tổng quát**, nhấn nút **Chạy** / **Dừng** / **Tạm ngưng** / **Khôi phục**.

Sửa cấu hình tác vụ

Để sửa cấu hình của một tác vụ cục bộ:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, mở thư mục với tên của nhóm quản trị chứa máy khách liên quan.
3. Trong không gian làm việc, chọn thẻ **Các thiết bị**.
4. Chọn máy tính mà bạn muốn thiết lập cấu hình ứng dụng.
5. Phải chuột để hiển thị menu ngữ cảnh của máy khách và chọn **Thuộc tính**.
   Một cửa sổ thuộc tính máy khách sẽ được mở ra.
6. Lựa chọn mục **Tác vụ**.
   Một danh sách tác vụ cục bộ sẽ được hiển thị ở phần bên phải của cửa sổ.
7. Chọn tác vụ cục bộ cần thiết trong danh sách tác vụ cục bộ.
8. Mở cửa sổ **Thuộc tính: <Tên chính sách>** sử dụng một trong những phương pháp sau đây:
   - Trong menu ngữ cảnh của chính sách, chọn **Thuộc tính**.
   - Nhấn vào liên kết **Thiết lập chính sách** được đặt ở phần bên phải của không gian làm việc của Bảng điều khiển Quản trị.
9. Trong cửa sổ **Thuộc tính:<Tên tác vụ cục bô>**, chọn mục **Cấu hình**.
10. Sửa cấu hình tác vụ cục bộ.

11. Để lưu thay đổi, trong cửa sổ **Thuộc tính: <Tên tác vụ cục bộ>**, nhấn **OK**.

12. Để lưu thay đổi, trong cửa sổ **Thuộc tính: <Tên tác vụ cục bộ>**, nhấn **OK**.

Để sửa cấu hình của một tác vụ nhóm:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Trong thư mục **Quản lý thiết bị**, mở thư mục với tên của nhóm quản trị liên quan.
3. Chọn thẻ **Tác vụ** trong không gian làm việc.
   Các tác vụ nhóm sẽ được hiển thị trong không gian làm việc của Bảng điều khiển Quản trị.
4. Chọn tác vụ nhóm cần thiết.
5. Mở cửa sổ **Thuộc tính: <Tên chính sách>** sử dụng một trong những phương pháp sau đây:
   - Trong menu ngữ cảnh của chính sách, chọn **Thuộc tính**.
   - Nhấn vào liên kết **Thiết lập chính sách** được đặt ở phần bên phải của không gian làm việc của Bảng điều khiển Quản trị.
6. Trong cửa sổ **Thuộc tính: <Tên tác vụ nhóm>**, chọn mục **Cấu hình**.
7. Sửa cấu hình tác vụ nhóm.
8. Để lưu thay đổi, trong cửa sổ **Thuộc tính: <Tên tác vụ nhóm>**, nhấn **OK**.

Để sửa cấu hình của một tác vụ cho các máy tính được chọn:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Trong thư mục **Tác vụ** của cây Bảng điều khiển Quản trị, chọn tác vụ cho các máy tính được lựa chọn có cấu hình mà bạn muốn sửa.
3. Mở cửa sổ **Thuộc tính: <Tên chính sách>** sử dụng một trong những phương pháp sau đây:
   - Trong menu ngữ cảnh của chính sách, chọn **Thuộc tính**.
   - Nhấn vào liên kết **Thiết lập chính sách** được đặt ở phần bên phải của không gian làm việc của Bảng điều khiển Quản trị.
4. Trong cửa sổ **Thuộc tính:<Tên của tác vụ cho các máy tính được lựa chọn>**, chọn mục **Cấu hình**.
5. Sửa cấu hình tác vụ cho các máy tính được lựa chọn.
6. Để lưu thay đổi, trong cửa sổ **Thuộc tính: <Tên của tác vụ cho các máy tính được lựa chọn>**, nhấn **OK**.

Ngoại trừ mục **Cấu hình**, tất cả các mục trong cửa sổ thuộc tính tác vụ đều giống với những mục được sử dụng trong Kaspersky Security Center. Để xem mô tả chi tiết, vui lòng tham khảo *Hướng dẫn dành cho Quản trị viên Kaspersky Security Center*. Mục **Cấu hình** chứa cấu hình cụ thể của Kaspersky Endpoint Security 10 for Windows. Nội dung của nó tùy thuộc vào tác vụ được chọn hoặc loại tác vụ.

Quản lý chính sách

Phần này thảo luận về việc tạo và thiết lập các chính sách cho Kaspersky Endpoint Security. Để biết thêm thông tin về việc quản lý Kaspersky Endpoint Security thông qua các chính sách của Kaspersky Security Center, vui lòng tham khảo *Hướng dẫn dành cho Quản trị viên Kaspersky Security Center*.

Thông tin về các chính sách

Bạn có thể sử dụng các chính sách để áp dụng cấu hình Kaspersky Endpoint Security giống nhau cho tất cả các máy khách trong một nhóm quản trị.

Bạn có thể thay đổi cục bộ giá trị của các cấu hình được quy định bởi một chính sách cho các máy tính riêng lẻ trong một nhóm quản trị sử dụng Kaspersky Endpoint Security. Bạn có thể thay đổi cục bộ chỉ những cấu hình mà việc thay đổi chúng không bị nghiêm cấm bởi chính sách.

Việc liệu một cấu hình ứng dụng trên máy khách có thể được sửa hay không được xác định bởi trạng thái "khóa" của cấu hình đó trong một chính sách:

- Nếu cấu hình bị "khóa" (), bạn không thể sửa cục bộ giá trị của cấu hình này. Các giá trị cấu hình được quy định bởi chính sách sẽ được sử dụng cho tất cả các máy khách trong nhóm quản trị.
- Khi một cấu hình được "mở khóa" (), bạn có thể sửa cục bộ cấu hình đó. Một cấu hình được thiết lập cục bộ sẽ được áp dụng cho tất cả các máy khách trong cùng nhóm quản trị. Cấu hình được thiết lập bởi chính sách sẽ không được áp dụng.

Sau khi chính sách được áp dụng ở lần đầu tiên, cấu hình ứng dụng cục bộ sẽ thay đổi tùy theo cấu hình chính sách.

Quyền truy cập đến cấu hình chính sách (đọc, ghi, thực thi) được quy định cho mỗi người dùng có thể truy cập Máy chủ Quản trị Kaspersky Security Center và riêng biệt cho từng phạm vi chức năng của Kaspersky Endpoint Security. Để thiết lập quyền truy cập đến các cấu hình chính sách, vào mục **Bảo mật** của cửa sổ thuộc tính trong Máy chủ Quản trị Kaspersky Security Center.

Các phạm vi chức năng sau của Kaspersky Endpoint Security sẽ được nêu bật:

- Bảo vệ Chống Virus. Phạm vi chức năng này bao gồm Chống virus cho tập tin, Chống virus cho thư điện tử, Chống virus cho web, Chống virus cho tin nhắn, Quét lỗ hổng bảo mật, và tác vụ quét.
- Kiểm soát Khởi động Ứng dụng. Phạm vi chức năng này bao gồm thành phần Kiểm soát khởi động ứng dụng.
- Kiểm soát Thiết bị. Phạm vi chức năng này bao gồm thành phần Kiểm soát thiết bị.
- Mã hóa. Phạm vi chức năng này bao gồm các thành phần mã hóa ổ cứng, tập tin và thư mục.
- Vùng tin tưởng. Phạm vi chức năng này bao gồm Vùng tin tưởng.
- Kiểm soát Web. Phạm vi chức năng này bao gồm thành phần Kiểm soát web.
- Ngăn chặn xâm nhập. Phạm vi chức năng này bao gồm Giám sát Hoạt động Ứng dụng, Giám sát Lỗ hổng bảo mật, Tường lửa, Ngăn chặn Tấn công Mạng và Kiểm soát Đặc quyền Ứng dụng.

- Chức năng cơ bản. Phạm vi chức năng này bao gồm các cấu hình ứng dụng chung không được quy định cho các phạm vi chức năng khác, bao gồm: giấy phép, cấu hình KSN, tác vụ lưu kho, cơ sở dữ liệu ứng dụng và các tác vụ cập nhật mô-đun, Tự bảo vệ, cấu hình ứng dụng nâng cao, báo cáo và lưu trữ, cấu hình mật khẩu bảo vệ, và cấu hình giao diện ứng dụng.

Bạn có thể thực hiện các hành động sau với một chính sách:

- Tạo một chính sách.
- Sửa cấu hình chính sách.

  Nếu tài khoản người dùng mà bạn sử dụng để truy cập Máy chủ Quản trị không có quyền sửa cấu hình của một số phạm vi chức năng nhất định, cấu hình của các phạm vi chức năng này sẽ không thể được sửa.

- Xóa một chính sách.
- Thay đổi trạng thái của chính sách.

Để biết thêm thông tin về việc sử dụng các chính sách không liên quan đến Kaspersky Endpoint Security, vui lòng tham khảo *Hướng dẫn dành cho Quản trị viên Kaspersky Security Center*.

Tạo một chính sách

Để tạo một chính sách:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Thực hiện một trong các thao tác sau:
   - Chọn thư mục **Quản lý thiết bị** trong cây Bảng điều khiển Quản trị nếu bạn muốn tạo một chính sách cho tất cả các máy tính được quản lý bởi Kaspersky Security Center.
   - Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, chọn thư mục với tên của nhóm quản trị chứa máy khách liên quan.
3. Trong không gian làm việc, chọn thẻ **Chính sách**.
4. Thực hiện một trong các thao tác sau:
   - Nhấn nút **Tạo chính sách**.
   - Nhấn phải chuột để mở menu ngữ cảnh và chọn **Tạo** Chính sách.

   Trình hướng dẫn Chính sách sẽ được bắt đầu.
5. Làm theo chỉ dẫn của Trình hướng dẫn Chính sách.

Sửa cấu hình chính sách

Để sửa cấu hình chính sách:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Trong thư mục **Quản lý thiết bị** của cây Bảng điều khiển Quản trị, mở thư mục với tên của nhóm quản trị mà bạn muốn sửa cấu hình chính sách.
3. Trong không gian làm việc, chọn thẻ **Chính sách**.
4. Chọn chính sách cần thiết.
5. Mở cửa sổ **Thuộc tính: <Tên chính sách>** sử dụng một trong những phương pháp sau đây:
   - Trong menu ngữ cảnh của chính sách, chọn **Thuộc tính**.
   - Nhấn vào liên kết **Thiết lập chính sách** được đặt ở phần bên phải của không gian làm việc của Bảng điều khiển Quản trị.

   Cấu hình chính sách Kaspersky Endpoint Security 10 for Windows bao gồm cấu hình của các thành phần và cấu hình ứng dụng. Các mục **Bảo vệ Chống virus** và **Bảng kiểm soát** của cửa sổ **Thuộc tính: <Tên chính sách>** hiển thị cấu hình của thành phần bảo vệ và kiểm soát, mục **Mã hóa Dữ liệu** hiển thị cấu hình mã hóa cho các tập tin và thư mục, còn mục **Cấu hình nâng cao** hiển thị cấu hình của ứng dụng.

   Để bật hiển thị cấu hình mã hóa dữ liệu và cấu hình của thành phần kiểm soát trong cấu hình chính sách, bạn phải chọn các hộp kiểm tương ứng trong cửa sổ **Cấu hình giao diện** của Kaspersky Security Center.
6. Sửa cấu hình chính sách.
7. Để lưu thay đổi của bạn, trong cửa sổ **Thuộc tính: <Tên chính sách>**, nhấn **OK**.

Chọn cấu hình được hiển thị trong chính sách Kaspersky Security Center

Để chọn cấu hình được hiển thị trong chính sách Kaspersky Security Center:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Trong menu ngữ cảnh của nút **Máy chủ Quản trị – <Tên máy tính>** của cây Bảng điều khiển Quản trị, chọn thẻ Xem → **Cấu hình giao diện**.

   Cửa sổ **Cấu hình giao diện** sẽ được mở ra.
3. Trong cửa sổ **Cấu hình giao diện**, chọn hộp kiểm đối diện các cấu hình cần được hiển thị trong cấu hình tạo chính sách Kaspersky Security Center và trong thuộc tính chính sách.
   - Chọn hộp kiểm **Hiển thị các thành phần kiểm soát đầu cuối** để cho phép hiển thị cấu hình thành phần kiểm soát trong cửa sổ của Trình hướng dẫn Chính sách Mới của Kaspersky Security Center và trong thuộc tính của chính sách.
   - Chọn hộp kiểm **Hiển thị mã hóa và bảo vệ dữ liệu** để cho phép hiển thị cấu hình mã hóa dữ liệu trong Trình hướng dẫn Chính sách Mới của Kaspersky Security Center và trong thuộc tính của chính sách.
4. Nhấn **OK**.

Gửi tin nhắn của người dùng đến máy chủ Kaspersky Security Center

Một người dùng có thể sẽ cần gửi thông điệp đến quản trị viên mạng doanh nghiệp cục bộ trong các trường hợp sau:

- Kiểm soát Thiết bị đã chặn truy cập đến thiết bị.

  Mẫu thông điệp yêu cầu truy cập một thiết bị bị chặn có thể được sử dụng trong giao diện Kaspersky Endpoint Security trong mục Kiểm soát Thiết bị.

- Kiểm soát Khởi động Ứng dụng đã chặn việc khởi động của một ứng dụng.

  Mẫu thông điệp yêu cầu cho phép khởi động một ứng dụng bị chặn có thể được sử dụng trong giao diện Kaspersky Endpoint Security trong mục Kiểm soát Khởi động Ứng dụng.

- Kiểm soát web đã chặn truy cập đến một tài nguyên web.

  Mẫu thông điệp yêu cầu truy cập một tài nguyên web bị chặn có thể được sử dụng trong giao diện Kaspersky Endpoint Security trong mục Kiểm soát web.

Phương thức được sử dụng để gửi tin nhắn và lựa chọn mẫu tin nhắn tùy thuộc vào việc liệu có một chính sách Kaspersky Security Center đang hoạt động trên máy tính cài đặt Kaspersky Endpoint Security hay không, và liệu có một kết nối với Máy chủ Quản trị của Kaspersky Security Center hay không. Các tình huống sau có thể xảy ra:

- Nếu chính sách Kaspersky Security Center đang không chạy trên máy tính cài đặt Kaspersky Security Center, tin nhắn của người dùng sẽ được gửi đến quản trị viên mạng máy tính cục bộ qua email.

  Trường tin nhắn sẽ được điền giá trị các trường từ mẫu tin nhắn, được quy định trong giao diện cục bộ của Kaspersky Endpoint Security.

- Nếu chính sách Kaspersky Security Center đang chạy trên máy tính cài đặt Kaspersky Security Center, các tin nhắn tiêu chuẩn sẽ được gửi đến Máy chủ Quản trị của Kaspersky Security Center.

  Trong trường hợp này, tin nhắn của người dùng có thể được xem trong kho lưu trữ sự kiện của Kaspersky Security Center. Trường tin nhắn sẽ được điền giá trị các trường từ mẫu tin nhắn, được quy định trong chính sách Kaspersky Security Center.

- Nếu chính sách ngoài văn phòng của Kaspersky Security Center đang được chạy trên máy tính cài đặt Kaspersky Endpoint Security, phương thức được sử dụng để gửi tin nhắn sẽ tùy thuộc vào việc liệu có một kết nối với Kaspersky Security Center hay không.

  - Nếu một kết nối với Kaspersky Security Center được thiết lập, Kaspersky Endpoint Security sẽ gửi tin nhắn tiêu chuẩn đến Máy chủ Quản trị của Kaspersky Security Center.

  - Nếu không có kết nối với Kaspersky Security Center, tin nhắn của người dùng sẽ được gửi đến quản trị viên mạng máy tính cục bộ qua email.

  Trong cả hai trường hợp, trường tin nhắn sẽ được điền giá trị các trường từ mẫu tin nhắn, được quy định trong chính sách Kaspersky Security Center.

Xem tin nhắn của người dùng trong kho lưu trữ sự kiện của Kaspersky Security Center

Các thành phần Kiểm soát ứng dụng khởi động, Kiểm soát Thiết bị và Kiểm soát web cho phép người dùng LAN với máy tính cài đặt Kaspersky Endpoint Security có thể gửi tin nhắn đến quản trị viên.

Một người dùng có thể gửi các thông điệp đến quản trị viên bằng hai cách:

- Dưới dạng một sự kiện trong kho lưu trữ sự kiện của Kaspersky Security Center.

  Sự kiện của người dùng sẽ được gửi đến kho lưu trữ sự kiện Kaspersky Security Center nếu ứng dụng Kaspersky Endpoint Security được cài đặt trên máy tính của người dùng đang hoạt động với một chính sách còn hiệu lực.

- Dưới dạng một email.

  Thông tin của người dùng sẽ được gửi qua email nếu ứng dụng Kaspersky Endpoint Security được cài đặt trên máy tính của người dùng đang không sử dụng một chính sách, hoặc đang sử dụng một chính sách ngoài văn phòng.

Để xem tin nhắn của người dùng trong kho lưu trữ sự kiện của Kaspersky Security Center:

1. Mở Bảng điều khiển Quản trị của Kaspersky Security Center.
2. Trong nút **Máy chủ Quản trị** của cây Bảng điều khiển Quản trị, chọn thẻ **Sự kiện**.

   Không gian làm việc của Kaspersky Security Center sẽ hiển thị tất cả các sự kiện xảy ra trong quá trình hoạt động của Kaspersky Endpoint Security, bao gồm các thông điệp được gửi đến quản trị viên từ người dùng mạng LAN.
3. Để thiết lập bộ lọc sự kiện, trong danh sách thả xuống **Chọn sự kiện**, chọn **Yêu cầu của người dùng**.
4. Chọn tin nhắn để gửi đến quản trị viên.
5. Mở ra cửa sổ **Cấu hình sự kiện** bằng một trong các cách sau:

   - Phải chuột vào sự kiện. Trong menu ngữ cảnh được mở ra, chọn **Thuộc tính**.
   - Nhấn vào nút **Mở cửa sổ thuộc tính sự kiện** ở phần bên phải của không gian làm việc của Bảng điều khiển Quản trị.

Tham gia Kaspersky Security Network

Mục này chứa thông tin về việc tham gia Kaspersky Security Network và chỉ dẫn cách để bật hoặc tắt việc sử dụng Kaspersky Security Network.

Thông tin về việc tham gia Kaspersky Security Network

Để bảo vệ máy tính của bạn một cách hiệu quả hơn, Kaspersky Endpoint Security sẽ sử dụng dữ liệu thu được từ người dùng trên khắp thế giới. *Kaspersky Security Network* được thiết kế để thu thập những dữ liệu này.

Kaspersky Security Network (KSN) là một hạ tầng dịch vụ đám mây cung cấp truy cập đến Cơ sở Tri thức trực tuyến của Kaspersky, có chứa thông tin về danh tiếng tập tin, tài nguyên web và phần mềm. Việc sử dụng dữ liệu từ Kaspersky Security Network đảm bảo thời gian phản ứng nhanh hơn cho Kaspersky Endpoint Security khi gặp phải các mối đe dọa mới, cải thiện hiệu năng của một số thành phần bảo vệ, và làm giảm nguy cơ phát hiện sai.

Tùy thuộc vào vị trí của cơ sở hạ tầng, sẽ có dịch vụ KSN Toàn cầu (cơ sở hạ tầng được lưu trữ bởi các máy chủ Kaspersky) và dịch vụ KSN Tư nhân (cơ sở hạ tầng được lưu trữ bởi các máy chủ thuộc bên thứ ba, ví dụ trên mạng của nhà cung cấp dịch vụ Internet).

Sau khi thay đổi giấy phép, hãy gửi chi tiết của khóa mới đến nhà cung cấp dịch vụ để có thể sử dụng KSN Tư nhân. Nếu không, việc trao đổi dữ liệu với KSN sẽ không thể được thực hiện.

Nhờ những người dùng tham gia KSN, Kaspersky có thể kịp thời nhận thông tin về các loại và nguồn gốc của mối đe dọa, phát triển các giải pháp để vô hiệu hóa chúng, và giảm thiểu lỗi phát hiện sai được hiển thị bởi các thành phần ứng dụng.

Trong quá trình tham gia KSN, ứng dụng sẽ tự động gửi số liệu thống kê được tạo trong hoạt động của ứng dụng đến KSN. Ứng dụng cũng có thể gửi một số tập tin nhất định (hoặc các phần của tập tin) mà tin tặc có thể sử dụng để gây hại cho máy tính hoặc dữ liệu đến Kaspersky để được kiểm tra thêm.

Sẽ không có dữ liệu cá nhân nào được thu thập, xử lý hay lưu trữ. Để biết thêm chi tiết về việc gửi số liệu thống kê được tạo trong quá trình tham gia KSN đến Kaspersky, và về việc lưu trữ cũng như tiêu hủy các thông tin đó, hãy tham khảo Tuyên bố Kaspersky Security Network và website Kaspersky. Tập tin ksn_<language ID>.txt chứa văn bản của Tuyên bố Kaspersky Security Network cũng được bao gồm trong gói phân phối ứng dụng.

Để giảm thiểu tải lên máy chủ KSN, Kaspersky có thể phát hành các cơ sở dữ liệu chống virus cho ứng dụng tạm thời tắt hoặc hạn chế một phần các yêu cầu đến Kaspersky Security Network. Trong trường hợp này, trạng thái kết nối đến KSN có thể được hiển thị là *Được bật với hạn chế*.

Máy tính của người dùng được quản lý bởi Máy chủ Quản trị của Kaspersky Security Center có thể tương tác với KSN thông qua dịch vụ KSN Proxy.

Dịch vụ KSN Proxy cung cấp các chức năng sau:

- Máy tính của người dùng có thể truy vấn KSN và gửi thông tin đến KSN mà không cần có truy cập trực tiếp đến Internet.
- KSN Proxy sẽ lưu lại dữ liệu được xử lý, giảm thiểu tải lên kết nối với mạng bên ngoài và tăng tốc độ nhận thông tin được yêu cầu bởi máy tính của người dùng.

Chi tiết bổ sung về dịch vụ KSN Proxy có thể được tham khảo trong *Hướng dẫn dành cho Quản trị viên Kaspersky Security Center*.

Cấu hình dịch vụ KSN Proxy có thể được thiết lập trong thuộc tính của chính sách *Kaspersky Security Center*.

Việc tham gia Kaspersky Security Network là tự nguyện. Ứng dụng sẽ mời người dùng tham gia KSN trong lần thiết lập ứng dụng ban đầu. Người dùng có thể bắt đầu hoặc ngừng tham gia KSN tại bất cứ thời điểm nào.

Bật và tắt việc sử dụng Kaspersky Security Network

Để bật hoặc tắt việc sử dụng Kaspersky Security Network:

1. Mở cửa sổ cấu hình ứng dụng.
2. Ở phần bên trái của cửa sổ, trong mục **Cấu hình nâng cao**, chọn mục con **Cấu hình KSN**.
   Cấu hình Kaspersky Security Network được hiển thị ở phần bên phải của cửa sổ.
3. Thực hiện một trong các thao tác sau:
   - Nếu bạn muốn bật Kaspersky Security Network, chọn hộp kiểm **Tôi chấp nhận tuyên bố KSN và các điều khoản tham gia**.
   - Nếu bạn muốn tắt Kaspersky Security Network, xóa hộp kiểm **Tôi chấp nhận tuyên bố KSN và các điều khoản tham gia**.
4. Để lưu lại các thay đổi, nhấn nút **Lưu**.

Kiểm tra kết nối đến Kaspersky Security Network

Để kiểm tra kết nối đến Kaspersky Security Network:

1. Mở cửa sổ chính của ứng dụng.
2. Ở phía trên của cửa sổ, bấm vào nút **Kaspersky Security Network**.
   Cửa sổ **Kaspersky Security Network** sẽ được mở ra.
   Phần bên trái của cửa sổ **Kaspersky Security Network** hiển thị chế độ kết nối đến Kaspersky Security Network dưới dạng một nút **KSN** tròn:
   - Nếu Kaspersky Endpoint Security không được kết nối đến Kaspersky Security Network, nút **KSN** sẽ có màu xám. Trạng thái được hiển thị dưới nút **KSN** sẽ là *Tắt*.
   - Nếu Kaspersky Endpoint Security được kết nối đến Kaspersky Security Network và máy chủ KSN đang khả dụng, nút **KSN** sẽ có màu xanh. Thông tin sau sẽ được hiển thị dưới nút **KSN**: Trạng thái

Bật, kiểu KSN được sử dụng – **KSN Tư nhân** hoặc **KSN Toàn cầu**, cùng ngày và giờ của lần đồng bộ gần nhất với các máy chủ KSN. Phần bên phải của cửa sổ hiển thị thông số về danh tiếng của các tập tin, tài nguyên web và phần mềm.

Kaspersky Endpoint Security sẽ thu thập dữ liệu thống kê về việc sử dụng KSN khi bạn mở cửa sổ **Kaspersky Security Network**. Số liệu thống kê không được cập nhật trong thời gian thực.

- Nếu Kaspersky Endpoint Security được kết nối đến Kaspersky Security Network nhưng máy chủ KSN đang không khả dụng, nút **KSN** sẽ có màu đỏ. Trạng thái được hiển thị dưới nút **KSN** sẽ là *Bật*.

  Nếu thời gian đồng bộ gần nhất với các máy chủ KSN là hơn 15 phút, hoặc có trạng thái *Không xác định*, điều này có nghĩa máy chủ KSN đang không khả dụng. Trong tình huống này, bạn được khuyến nghị liên hệ với bộ phận Hỗ trợ kỹ thuật hoặc nhà cung cấp dịch vụ của mình.

  Một kết nối đến các máy chủ Kaspersky Security Network có thể bị mất do các lý do sau:

  - Máy tính không kết nối đến Internet.
  - Ứng dụng chưa được kích hoạt hoặc giấy phép đã hết hạn.
  - Các vấn đề liên quan đến khóa đã được phát hiện (ví dụ, khóa đã được cho vào danh sách đen).

Kiểm tra danh tiếng của một tập tin trong Kaspersky Security Network

Dịch vụ KSN cho phép bạn truy hồi thông tin về các ứng dụng được bao gồm trong cơ sở dữ liệu danh tiếng Kaspersky. Việc này cho phép quản lý linh hoạt các chính sách khởi động ứng dụng ở cấp độ công ty, qua đó ngăn cản việc khởi động các phần mềm quảng cáo và những chương trình khác có thể được sử dụng bởi bọn tội phạm để phá hoại máy tính hoặc dữ liệu cá nhân của bạn.

Để kiểm tra danh tiếng của một tập tin trong Kaspersky Security Network:

1. Nhấn phải chuột để gọi menu ngữ cảnh của tập tin mà bạn muốn kiểm tra danh tiếng.
2. Chọn **Kiểm tra danh tiếng trong KSN**.

Tùy chọn này có thể được sử dụng nếu bạn đã chấp nhận các điều khoản của Tuyên bố Kaspersky Security Network.

Việc này mở ra cửa sổ **<Tên tập tin> - Danh tiếng trong KSN**. Cửa sổ **<Tên tập tin> - Danh tiếng trong KSN** hiển thị các thông tin sau về tập tin được kiểm tra:

- **Đường dẫn**. Đường dẫn lưu tập tin lên ổ đĩa.
- **Phiên bản**. Phiên bản ứng dụng (thông tin chỉ được hiển thị cho các tập tin thực thi).
- **Chữ ký điện tử**. Sự hiện diện của một chữ ký điện tử trong tập tin.
- **Chữ ký**. Ngày chứng chỉ được ký với một chữ ký điện tử.

- **Ngày khởi tạo**. Ngày tạo tập tin.
- **Thay đổi**. Ngày sửa đổi gần nhất của tập tin.
- **Dung lượng**. Không gian ổ đĩa được sử dụng bởi tập tin.
- Thông tin về số lượng người dùng tin tưởng tập tin hoặc chặn tập tin.

Tăng cường bảo vệ với Kaspersky Security Network

Kaspersky cung cấp một lớp bảo vệ bổ sung cho người dùng thông qua Kaspersky Security Network. Phương thức bảo vệ này được thiết kế để chống lại các mối đe dọa cao cấp thường trực và các cuộc tấn công zero-day. Các công nghệ đám mây tích hợp và trình độ của các chuyên gia virus Kaspersky khiến Kaspersky Endpoint Security là lựa chọn hàng đầu để bảo vệ chống lại những mối đe dọa mạng tinh tế nhất.

Chi tiết về tính năng bảo vệ được tăng cường của Kaspersky Endpoint Security có thể được tìm hiểu trên website Kaspersky.

Các nguồn thông tin về ứng dụng

Trang Kaspersky Endpoint Security trên website Kaspersky

Trên Trang Kaspersky Endpoint Security, bạn có thể xem thông tin chung về ứng dụng cũng như các chức năng và tính năng của ứng dụng đó.

Trang Kaspersky Endpoint Security có chứa một liên kết đến cửa hàng trực tuyến. Ở đó bạn có thể mua hoặc gia hạn ứng dụng.

Trang Kaspersky Endpoint Security trong Cơ sở Tri thức

Cơ sở Tri thức là một phần trên website Hỗ trợ Kỹ thuật.

Trên trang Kaspersky Endpoint Security trong Cơ sở Tri thức, bạn có thể đọc các bài viết cung cấp thông tin hữu ích, khuyến nghị và câu trả lời cho các câu hỏi thường gặp về cách mua, cài đặt và sử dụng ứng dụng.

Các bài viết Kiến thức cơ bản có thể trả lời những câu hỏi không chỉ liên quan đến Kaspersky Endpoint Security, mà còn các ứng dụng khác của Kaspersky. Các bài viết trong Cơ sở Tri thức cũng có thể chứa tin tức từ nhóm Hỗ trợ Kỹ thuật.

Thảo luận về phần mềm Kaspersky trên diễn đàn

Nếu bạn không cần được giải đáp thắc mắc ngay, bạn có thể thảo luận với các chuyên gia của Kaspersky và những người dùng khác trên diễn đàn của chúng tôi.

Trong diễn đàn này bạn có thể xem các chủ đề hiện tại, để lại ý kiến của bạn, và tạo các chủ đề thảo luận mới.

Liên hệ với Hỗ trợ kỹ thuật

Phần này mô tả cách để nhận hỗ trợ kỹ thuật và các điều khoản cung cấp dịch vụ này.

Làm thế nào để được hỗ trợ kỹ thuật

Nếu bạn không tìm thấy giải pháp cho vấn đề của mình trong tài liệu về ứng dụng hoặc trong các nguồn thông tin về ứng dụng, chúng tôi khuyên bạn nên liên hệ với bộ phận Hỗ trợ kỹ thuật. Các chuyên gia Hỗ trợ Kỹ thuật sẽ trả lời bất kỳ câu hỏi nào mà bạn có về cài đặt và sử dụng ứng dụng.

Hỗ trợ kỹ thuật chỉ được cung cấp cho những người sử dụng đã một giấy phép thương mại. Những người dùng có một giấy phép dùng thử sẽ không được hỗ trợ kỹ thuật.

Trước khi liên hệ với bộ phận Hỗ trợ Kỹ thuật, vui lòng đọc quy tắc hỗ trợ.

Bạn có thể liên hệ với dịch vụ Hỗ trợ kỹ thuật bằng những cách sau:

- Bằng cách gọi đến Hỗ trợ Kỹ thuật qua điện thoại
- Gửi yêu cầu đến bộ phận Hỗ trợ kỹ thuật Kaspersky qua cổng thông tin Kaspersky CompanyAccount.

Hỗ trợ kỹ thuật qua điện thoại

Bạn có thể gọi cho các đại diện Hỗ trợ kỹ thuật từ hầu hết các khu vực trên thế giới. Bạn có thể tìm thông tin về cách nhận hỗ trợ kỹ thuật trong khu vực của bạn và thông tin liên hệ của bộ phận Hỗ trợ Kỹ thuật trên website Hỗ trợ Kỹ thuật của Kaspersky.

Trước khi liên hệ với bộ phận Hỗ trợ Kỹ thuật, vui lòng đọc quy tắc hỗ trợ.

Hỗ trợ kỹ thuật qua Kaspersky CompanyAccount

Kaspersky CompanyAccount là một cổng thông tin cho các công ty sử dụng ứng dụng của Kaspersky. Cổng thông tin Kaspersky CompanyAccount được thiết kế để hỗ trợ tương tác giữa người dùng và các chuyên gia Kaspersky qua các yêu cầu điện tử. Bạn có thể sử dụng cổng thông tin Kaspersky CompanyAccount để theo dõi trạng thái của các yêu cầu điện tử của mình và lưu lại một lịch sử các yêu cầu này.

Bạn có thể đăng ký tất cả các nhân viên của doanh nghiệp mình trong một tài khoản duy nhất trên Kaspersky CompanyAccount. Một tài khoản duy nhất sẽ cho phép bạn quản lý tập trung các yêu cầu điện tử từ những nhân viên được đăng ký đến Kaspersky, đồng thời quản lý các đặc quyền của những nhân viên này thông qua Kaspersky CompanyAccount.

Cổng thông tin Kaspersky CompanyAccount được cung cấp bằng các ngôn ngữ sau:

- Tiếng Anh
- Tiếng Tây Ban Nha
- Tiếng Ý
- Tiếng Đức
- Tiếng Ba Lan
- Tiếng Bồ Đào Nha
- Tiếng Nga
- Tiếng Pháp
- Tiếng Nhật

Để tìm hiểu thêm về Kaspersky CompanyAccount, hãy truy cập website Hỗ trợ kỹ thuật.

Thu thập thông tin về Hỗ trợ Kỹ thuật

Sau khi bạn đã thông báo với các chuyên gia Hỗ trợ kỹ thuật của Kaspersky về vấn đề của mình, họ có thể yêu cầu bạn tạo một *tập tin dấu vết*. Tập tin dấu vết cho phép bạn truy vết từng bước trong quá trình thực hiện lệnh của ứng dụng và xác định giai đoạn hoạt động của ứng dụng đã xảy ra lỗi.

Các chuyên gia Hỗ trợ kỹ thuật cũng có thể yêu cầu thêm thông tin về hệ điều hành, các tiến trình đang chạy trên máy tính, báo cáo chi tiết về hoạt động của các thành phần ứng dụng, và tập tin kết xuất lỗi sập ứng dụng.

Bạn có thể thu thập những thông tin cần thiết với sự trợ giúp của Kaspersky Endpoint Security. Những thông tin được thu thập có thể được lưu trên ổ cứng và được tải lên tại một thời điểm thuận tiện cho bạn.

Khi chạy chẩn đoán, các chuyên gia Hỗ trợ kỹ thuật có thể yêu cầu bạn thay đổi cấu hình của ứng dụng bằng cách:

- Kích hoạt chức năng thu thập thông tin chẩn đoán mở rộng.
- Tinh chỉnh cấu hình của các thành phần ứng dụng riêng lẻ, không được cung cấp qua các yếu tố giao diện người dùng tiêu chuẩn.
- Thay đổi cấu hình lưu trữ và truyền tải thông tin chẩn đoán được thu thập.
- Thiết lập việc theo dõi và ghi lại lưu lượng mạng.

Các chuyên gia Hỗ trợ kỹ thuật sẽ cung cấp tất cả thông tin cần thiết để thực hiện những hoạt động này (mô tả trình tự các bước, cấu hình cần được thay đổi, các tập tin thiết lập, kịch bản, chức năng dòng lệnh bổ sung, gỡ lỗi cho các mô-đun, các tiện ích có chức năng đặc biệt, v.v...) và thông báo cho bạn về phạm vi dữ liệu được thu thập vì mục đích gỡ lỗi. Thông tin chẩn đoán mở rộng được thu thập sẽ được lưu trên máy tính của người dùng. Dữ liệu được thu thập sẽ không tự động được truyền tải đến Kaspersky.

Cấu hình được sử dụng để xác định địa chỉ của máy chủ kết xuất để gửi các tập tin kết xuất đến Kaspersky sẽ được lưu trên máy tính của người dùng. Nếu cần thiết, các giá trị của những cấu hình này có thể được sửa trong khóa registry của hệ điều hành `"DumpServerConfigUrl"="https://dmpcfg.kaspersky-labs.com/dumpserver/config.xml"`.

Các hoạt động được liệt kê ở trên chỉ nên được thực hiện với sự giám sát của các chuyên gia Hỗ trợ kỹ thuật bằng cách làm theo hướng dẫn của họ. Những thay đổi không được giám sát đến cấu hình ứng dụng, được thực hiện theo những cách không được mô tả trong Hướng dẫn dành cho Quản trị viên hoặc hướng dẫn của chuyên gia Hỗ trợ kỹ thuật có thể làm chậm hoặc sập hệ điều hành, ảnh hưởng đến chức năng bảo mật máy tính, hoặc gây hại đến sự sẵn có và tính toàn vẹn của dữ liệu được xử lý.

Tạo một tập tin dấu vết

Để tạo một tập tin dấu vết:

1. Mở cửa sổ chính của ứng dụng.
2. Trong cửa sổ chính của ứng dụng, nhấn nút .
   Cửa sổ **Hỗ trợ** sẽ được mở ra.
3. Trong cửa sổ **Hỗ trợ**, nhấn nút **Ghi nhận dấu vết hệ thống**.
   Cửa sổ **Thông tin hỗ trợ kỹ thuật** sẽ được mở ra.
4. Để bắt đầu tiến trình ghi nhận dấu vết, chọn hộp kiểm **Cho phép dấu vết**.
5. Trong danh sách thả xuống **Mức độ**, chọn cấp độ ghi nhận dấu vết.
   Bạn nên xác định rõ cấp độ ghi nhận dấu vết cần thiết với chuyên gia Hỗ trợ kỹ thuật. Nếu không có hướng dẫn từ Hỗ trợ kỹ thuật, đặt cấp độ ghi nhận dấu vết là **Bình thường (500)**.
6. Tái tạo lại tình huống xảy ra vấn đề.
7. Để dừng tiến trình ghi nhận dấu vết, quay lại cửa sổ **Thông tin hỗ trợ kỹ thuật** và xóa hộp kiểm **Cho phép dấu vết**.

Sau khi đã tạo ra tập tin dấu vết, bạn có thể tiếp tục tải kết quả ghi nhận dấu vết lên máy chủ Kaspersky.

Nội dung và bộ nhớ của tập tin dấu vết

Người dùng phải chịu trách nhiệm cá nhân cho việc đảm bảo sự an toàn của dữ liệu được thu thập, cụ thể phải giám sát và hạn chế truy cập đến dữ liệu được thu thập trên máy tính cho đến khi nó được gửi đến Kaspersky.

Các tập tin dấu vết được lưu trữ trên máy tính của bạn dưới dạng sửa đổi không thể được đọc chừng nào ứng dụng còn đang được sử dụng, và sẽ bị xóa vĩnh viễn khi ứng dụng bị gỡ bỏ.

Các tập tin dấu vết được lưu trữ trong thư mục ProgramData\Kaspersky Lab .

Tập tin dấu vết có định dạng tên như sau: `KES<version number_dateXX.XX_timeXX.XX_pidXXX.><trace file type>.log.enc1`.

Tập tin dấu vết của Authentication Agent được lưu trữ trong thư mục System Volume Information và có tên như sau: `KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin`.

Bạn có thể xem dữ liệu được lưu trong các tập tin dấu vết. Vui lòng liên hệ với Hỗ trợ kỹ thuật của Kaspersky để được hướng dẫn cách xem dữ liệu.

Tất cả các tập tin dấu vết đều chứa các dữ liệu chung như sau:

- Thời gian sự kiện.
- Số hiệu của luồng thực thi.

  Tập tin dấu vết của Authentication Agent không chứa thông tin này.

- Thành phần ứng dụng đã gây ra sự kiện.
- Cấp độ nghiêm trọng của sự kiện (sự kiện thông tin, cảnh báo, sự kiện thiết yếu, lỗi).
- Mô tả về sự kiện liên quan đến việc thực thi lệnh bởi một thành phần của ứng dụng và kết quả thực thi lệnh này.

Nội dung của các tập tin dấu vết SRV.log, GUI.log, và ALL.log

Các tập tin dấu vết SRV.log, GUI.log, và ALL.log có thể chứa các thông tin sau, ngoài dữ liệu chung:

- Dữ liệu cá nhân, bao gồm họ, tên và tên đệm, nếu các dữ liệu đó được bao gồm trong đường dẫn đến tập tin trên máy tính cục bộ.
- Tên người dùng và mật khẩu nếu chúng được truyền tải công khai. Dữ liệu này có thể được ghi lại trong các tập tin dấu vết trong tác vụ quét lưu lượng Internet. Lưu lượng chỉ được ghi lại trong các tập tin dấu vết từ trafmon2.ppl.
- Tên người dùng và mật khẩu nếu chúng được chứa trong các đầu mục HTTP.
- Tên của tài khoản Microsoft Windows nếu tên tài khoản được bao gồm trong một tên tập tin.
- Địa chỉ email hoặc địa chỉ web chứa tên tài khoản và mật khẩu của bạn nếu chúng được chứa trong tên của đối tượng được phát hiện.
- Các website mà bạn đã truy cập và trang web tái điều hướng từ những website này. Dữ liệu này được ghi vào các tập tin dấu vết khi ứng dụng quét các website.
- Địa chỉ máy chủ proxy, tên máy tính, cổng, địa chỉ IP, và tên người dùng được sử dụng để đăng nhập vào máy chủ proxy. Dữ liệu này được ghi vào các tập tin dấu vết nếu ứng dụng sử dụng một máy chủ proxy.
- Địa chỉ IP từ xa mà máy tính của bạn đã thiết lập kết nối đến đó.
- Tiêu đề thư, ID, tên người gửi và địa chỉ của trang web của người gửi thư trên một mạng xã hội. Dữ liệu này được ghi vào các tập tin dấu vết nếu thành phần Kiểm soát web được bật.

Nội dung của các tập tin dấu vết HST.log, BL.log, Dumpwriter.log, WD.log, AVPCon.dll.log

Ngoài dữ liệu chung, tập tin dấu vết HST.log chứa thông tin về việc thực thi một tác vụ cập nhật cơ sở dữ liệu và mô-đun ứng dụng.

Ngoài dữ liệu chung, tập tin dấu vết BL.log chứa thông tin về các sự kiện xảy ra trong quá trình hoạt động của ứng dụng, cũng như dữ liệu cần thiết để khắc phục các lỗi ứng dụng. Tập tin này được tạo nếu ứng dụng được khởi động với tham số avp.exe –bl.

Ngoài dữ liệu chung, tập tin dấu vết Dumpwriter.log chứa thông tin dịch vụ cần thiết để khắc phục các lỗi xảy ra khi tập tin kết xuất của ứng dụng được ghi.

Ngoài dữ liệu chung, tập tin dấu vết WD.log chứa thông tin về các sự kiện xảy ra trong quá trình hoạt động của dịch vụ avpsus, bao gồm các sự kiện cập nhật mô-đun ứng dụng.

Ngoài dữ liệu chung, tập tin dấu vết AVPCon.dll.log chứa thông tin về các sự kiện xảy ra trong quá trình hoạt động của mô-đun kết nối Kaspersky Security Center.

Nội dung của các tập tin dấu vết của tiện ích ứng dụng

Các tập tin dấu vết của tiện ích ứng dụng chứa những thông tin sau, ngoài dữ liệu chung:

- Tập tin dấu vết shellex.dll.log của tiện ích khởi động tác vụ quét từ menu ngữ cảnh chứa thông tin về việc thực thi tác vụ quét và dữ liệu cần thiết để gỡ lỗi cho tiện ích.
- Tập tin dấu vết mcou.OUTLOOK.EXE của tiện ích Chống virus cho thư điện tử có thể chứa các phần của email, bao gồm địa chỉ email.

Nội dung của tập tin dấu vết cho Authentication Agent

Ngoài dữ liệu chung, tập tin dấu vết của Authentication Agent chứa thông tin về hoạt động của Authentication Agent và các hoạt động được thực hiện bởi người dùng với Authentication Agent.

Bật hoặc tắt việc truyền tải các tập tin kết xuất và dấu vết đến Kaspersky

Để bật hoặc tắt việc truyền tải các tập tin kết xuất và dấu vết đến Kaspersky:

1. Mở cửa sổ cấu hình ứng dụng.
2. Ở phần bên trái của cửa sổ, chọn mục **Cấu hình nâng cao**.
   Cấu hình nâng cao của ứng dụng sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Trong mục **Chế độ hoạt động**, nhấn nút **Cấu hình**.
   Cửa sổ **Chế độ hoạt động** sẽ được mở ra.
4. Trong cửa sổ **Chế độ hoạt động**, chọn hộp kiểm **Cho phép ghi tập tin dump** để cho phép ứng dụng ghi các tập tin kết xuất ứng dụng.
5. Thực hiện một trong các thao tác sau:

- Chọn hộp kiểm **Gửi tập tin dump và dấu vết đến Kaspersky Lab** nếu bạn muốn ứng dụng hiển thị lời nhắc trong cửa sổ **Gửi thông tin Hỗ Trợ Kỹ Thuật đến máy chủ** để gửi các tập tin kết xuất và tập tin dấu vết đến Kaspersky để phân tích lý do xảy ra lỗi ứng dụng ở lần ứng dụng được khởi động tiếp theo.

- Nếu không, hãy xóa hộp kiểm **Gửi tập tin dump và dấu vết đến Kaspersky**.

6. Nhấn **OK** trong cửa sổ **Chế độ hoạt động**.

7. Để lưu lại các thay đổi, nhấn nút **Lưu** trong cửa sổ chính của ứng dụng.

Gửi các tập tin đến máy chủ Hỗ trợ kỹ thuật

Các tập tin chứa thông tin về hệ điều hành, tập tin dấu vết, và tập tin kết xuất phải được gửi đến các chuyên gia Hỗ trợ kỹ thuật của Kaspersky.

Để gửi các tập tin đến máy chủ Hỗ trợ kỹ thuật:

1. Khởi động lại Kaspersky Endpoint Security sau khi có bất kỳ lỗi nào trong quá trình hoạt động của ứng dụng.

   Việc này sẽ mở ra cửa sổ **Lần khởi chạy ứng dụng gần nhất đã thất bại**.

   > Cửa sổ **Lần khởi chạy ứng dụng gần nhất đã thất bại** sẽ mở ra mỗi khi Kaspersky Endpoint Security được khởi động (bao gồm sau khi bạn đã khởi động lại máy tính) cho đến khi bạn gửi các tập tin dấu vết hay tập tin kết xuất đến Hỗ trợ Kỹ thuật, hoặc đến khi bạn nhấn vào nút **Không gửi**.

2. Trong cửa sổ **Lần khởi chạy ứng dụng gần nhất đã thất bại**, mở danh sách các tập tin được tạo bằng cách nhấn nút **đây**.

3. Chọn hộp kiểm cạnh các tập tin mà bạn muốn gửi đến Hỗ trợ kỹ thuật.

4. Nhấn nút **Hiển thị nội dung bản tuyên bố**.

   Cửa sổ **Tuyên bố Cung cấp Dữ liệu** sẽ được mở ra.

5. Đọc văn bản của Tuyên bố Cung cấp Dữ liệu và nhấn nút **Đóng**.

6. Trong cửa sổ **Lần khởi chạy ứng dụng gần nhất đã thất bại**, chọn hộp kiểm **Tôi đồng ý với Tuyên bố Cung cấp Dữ liệu**.

7. Nhấn nút **Gửi**.

   Việc này sẽ mở ra cửa sổ **Số yêu cầu**.

8. Trong cửa sổ **Số yêu cầu**, nhập số hiệu đã được gán cho yêu cầu của bạn khi bạn liên hệ với Hỗ trợ kỹ thuật thông qua Kaspersky CompanyAccount.

9. Nhấn **OK**.

Chọn tập tin dữ liệu là dạng gói và gửi máy chủ dịch vụ Hỗ trợ kỹ thuật.

Bật và tắt tính năng bảo vệ các tập tin kết xuất và tập tin dấu vết

Các tập tin kết xuất và tập tin dấu vết chứa thông tin về hệ điều hành, cũng như dữ liệu bí mật của người dùng. Để ngăn chặn việc truy cập trái phép đến các dữ liệu này, bạn có thể bật tính năng bảo vệ các tập tin kết xuất và tập tin dấu vết.

Nếu tính năng bảo vệ các tập tin kết xuất và tập tin dấu vết được bật, các tập tin này chỉ có thể được truy cập bởi những người dùng sau:

- Các tập tin kết xuất có thể được truy cập bởi quản trị viên hệ thống và quản trị viên mạng cục bộ, và bởi người dùng đã bật tính năng ghi tập tin kết xuất và tập tin dấu vết.
- Các tập tin dấu vết chỉ có thể được truy cập bởi quản trị viên hệ thống và quản trị viên mạng cục bộ.

Để bật hoặc tắt tính năng bảo vệ các tập tin kết xuất và tập tin dấu vết:

1. Mở cửa sổ cấu hình ứng dụng.
2. Chọn mục **Cấu hình nâng cao** ở phía bên trái.
   Cấu hình của ứng dụng sẽ được hiển thị ở phần bên phải của cửa sổ.
3. Trong mục **Chế độ hoạt động**, nhấn nút **Cấu hình**.
   Cửa sổ **Chế độ hoạt động** sẽ được mở ra.
4. Thực hiện một trong các thao tác sau:
   - Chọn hộp kiểm **Cho phép bảo vệ các tập tin dump và dấu vết** nếu bạn muốn bật tính năng bảo vệ.
   - Xóa hộp kiểm **Cho phép bảo vệ các tập tin dump và dấu vết** nếu bạn muốn tắt tính năng bảo vệ.
5. Nhấn **OK** trong cửa sổ **Chế độ hoạt động**.
6. Để lưu lại các thay đổi, nhấn nút **Lưu** trong cửa sổ chính của ứng dụng.

Các tập tin kết xuất và tập tin dấu vết đã được ghi khi tính năng bảo vệ còn hoạt động sẽ vẫn được bảo vệ ngay cả khi chức năng này đã bị tắt.

Thuật ngữ

Authentication Agent

Một giao diện để vượt qua quy trình xác thực để truy cập các ổ cứng được mã hóa và nạp hệ điều hành sau khi ổ cứng hệ thống đã được mã hóa.

Bản vá

Một bổ sung nhỏ đến ứng dụng giúp sửa các lỗi được phát hiện trong quá trình hoạt động của ứng dụng, hoặc cài đặt các bản cập nhật.

Báo động giả

Một báo động giả xảy ra khi ứng dụng Kaspersky báo cáo một tập tin không bị nhiễm là có bị nhiễm virus bởi dấu hiệu của tập tin giống với một virus.

Cách ly

Kaspersky Endpoint Security sẽ đặt các tập tin có khả năng bị nhiễm vào thư mục này. Các tập tin cách ly được lưu trữ dưới dạng mã hóa.

Cập nhật

Quy trình thay thế hoặc thêm tập tin mới (cơ sở dữ liệu hoặc mô-đun ứng dụng) được truy hồi từ các máy chủ cập nhật của Kaspersky.

Cấu hình tác vụ

Cấu hình ứng dụng cụ thể cho từng loại tác vụ.

Cấu hình ứng dụng

Cấu hình ứng dụng phổ biến cho tất cả các loại tác vụ và quy định hoạt động tổng quát của ứng dụng, ví dụ như cấu hình hiệu năng ứng dụng, cấu hình báo cáo, và cấu hình sao lưu.

Chứng chỉ vân tay

Thông tin được sử dụng để xác định một khóa chứng chỉ. Một vân tay được tạo bằng cách áp dụng một chức năng mã băm mật mã vào giá trị của khóa.

Chứng nhận

Các tài liệu điện tử chứa khóa cá nhân và thông tin về chủ sở hữu của khóa và phạm vi khóa, và xác nhận rằng khóa công cộng thuộc về người chủ sở hữu. Chứng nhận phải được ký tên bởi trung tâm chứng nhận đã cấp nó.

Chứng nhận giấy phép

Một tài liệu mà Kaspersky chuyển đến người dùng cùng với tập tin key hoặc mã kích hoạt. Nó chứa thông tin về giấy phép được cấp cho người dùng.

Cơ sở dữ liệu chống virus

Cơ sở dữ liệu chứa thông tin về các mối đe dọa về bảo mật máy tính mà Kaspersky biết được tính đến thời điểm phát hành cơ sở dữ liệu diệt virus. Các chữ ký trong cơ sở dữ liệu chống virus giúp phát hiện mã độc trong các đối tượng được quét. Các cơ sở dữ liệu diệt virus được tạo bởi các chuyên gia của Kaspersky và được cập nhật hàng giờ.

Cơ sở dữ liệu về các địa chỉ web độc hại

Danh sách các địa chỉ web chứa nội dung có thể bị coi là nguy hiểm. Danh sách này được tạo bởi các chuyên gia Kaspersky. Danh sách được cập nhật thường xuyên và có trong gói phân phối ứng dụng Kaspersky.

Cơ sở dữ liệu về các địa chỉ web lừa đảo

Một danh sách các địa chỉ web mà các chuyên gia Kaspersky đã xác định là có liên quan đến lừa đảo. Cơ sở dữ liệu này được cập nhật thường xuyên và là một phần của gói phân phối ứng dụng Kaspersky.

Dạng chuẩn hóa của địa chỉ của một tài nguyên web

Dạng chuẩn hóa của địa chỉ tài nguyên web là một dạng văn bản địa chỉ tài nguyên web được nhận sau khi chuẩn hóa. Chuẩn hóa là quá trình mà qua đó dạng văn bản của địa chỉ tài nguyên web được thay đổi theo các quy tắc cụ thể (ví dụ, loại bỏ đăng nhập HTTP, mật khẩu, và cổng kết nối từ dạng văn bản của địa chỉ tài nguyên web; thêm vào đó, địa chỉ tài nguyên web sẽ được thay đổi từ dạng viết hoa xuống dạng viết thường).

Trong ngữ cảnh chống virus, mục đích của chuẩn hóa địa chỉ tài nguyên web là để tránh phải quét lặp lại các địa chỉ website khác nhau về cú pháp nhưng vẫn tương đương nhau về mặt vật lý.

Ví dụ:

Dạng phi chuẩn hóa của một địa chỉ: www.Example.com\.
Dạng chuẩn hóa của một địa chỉ: www.example.com.

Danh sách địa chỉ đen

Một danh sách địa chỉ email mà các email nhận từ đó đều bị chặn bởi ứng dụng Kaspersky, bất kể nội dung của email.

Di chuyển tập tin đến Cách ly

Một phương thức để xử lý tập tin có khả năng bị nhiễm, qua đó truy cập đến tập tin sẽ bị chặn và tập tin được di chuyển từ vị trí gốc của nó đến thư mục Cách ly, ở đó nó sẽ được lưu trữ dưới dạng mã hóa để loại trừ nguy cơ lây lan.

Dịch vụ mạng

Một nhóm tham số quy định hoạt động mạng. Đối với hoạt động mạng này, bạn có thể tạo một quy tắc mạng điều tiết hoạt động của Tường lửa.

Đối tượng OLE

Một tập tin đính kèm hoặc một tập tin được nhúng trong một tập tin khác. Ứng dụng Kaspersky cho phép quét các đối tượng OLE để phát hiện virus. Ví dụ, nếu bạn chèn một bảng Microsoft Office Excel® vào một tài liệu Microsoft Office Word, bảng này sẽ được quét như một đối tượng OLE.

Đơn vị cấp chứng nhận

Trung tâm chứng nhận đã cấp chứng nhận.

Đơn vị sở hữu chứng nhận

Người giữ khóa cá nhân được liên kết đến một chứng nhận. Đây có thể là một người dùng, ứng dụng, bất kỳ đối tượng ảo, máy tính, hoặc dịch vụ nào.

Khóa bổ sung

Một khóa chứng nhận quyền sử dụng ứng dụng nhưng hiện không được sử dụng.

Khóa kích hoạt

Một khóa hiện đang được sử dụng bởi ứng dụng.

Khử nhiễm

Một phương thức xử lý các đối tượng bị nhiễm giúp khôi phục một phần hay toàn bộ dữ liệu. Không phải đối tượng bị nhiễm nào cũng có thể được khử nhiễm.

Lừa đảo

Một loại gian lận Internet trong đó các email được gửi đi với mục đích đánh cắp dữ liệu bảo mật, hầu hết là dữ liệu tài chính.

Mã khai thác

Mã chương trình sử dụng một số lỗ hổng bảo mật trong hệ thống hay phần mềm. Mã khai thác thường được sử dụng để cài đặt phần mềm độc hại trên máy tính mà không có sự cho phép của người dùng.

Mặt nạ tập tin

Đại diện một tên tập tin và phần mở rộng bằng ký tự đại diện.

Các mặt nạ tập tin có thể chứa bất kỳ ký tự nào được cho phép trong tên tập tin, bao gồm các ký tự đại diện:

- ***** – Thay thế từ 0 ký tự - số ký tự bất kỳ.
- **?** – Thay thế một ký tự bất kỳ.

Hãy lưu ý rằng tên tập tin và phần mở rộng luôn được ngăn cách bởi một dấu chấm.

Máy chủ Quản trị

Một thành phần của Kaspersky Security Center lưu trữ tập trung thông tin về tất cả các ứng dụng Kaspersky được cài đặt trong mạng doanh nghiệp. Nó cũng có thể được sử dụng để quản lý các ứng dụng này.

Mô-đun Nền tảng Đáng Tin cậy

Một microchip được phát triển để cung cấp các chức năng cơ bản liên quan đến bảo mật (ví dụ, để lưu trữ các khóa mã hóa). Một Mô-đun Nền tảng Đáng Tin cậy thường được lắp trên bo mạch chủ máy tính và tương tác với tất cả các thành phần hệ thống khác qua bus phần cứng.

Mô-đun ứng dụng

Các tập tin được bao gồm trong tập tin cài đặt ứng dụng và thực hiện chức năng cốt lõi của ứng dụng. Một mô-đun thực thi riêng biệt tương ứng với từng loại tác vụ được thực hiện bởi ứng dụng (Bảo vệ trong Thời gian thực, Quét theo Yêu cầu, và Cập nhật). Khi bắt đầu một tác vụ quét toàn bộ máy tính từ cửa sổ chính của ứng dụng, bạn sẽ bắt đầu mô-đun của tác vụ này.

Network Agent

Một thành phần Kaspersky Security Center cho phép tương tác giữa Máy chủ Quản trị và các ứng dụng Kaspersky được cài đặt trên một nút mạng cụ thể (máy trạm hoặc máy chủ). Thành phần này là phổ biến trên tất cả các ứng dụng Kaspersky chạy Windows. Các phiên bản chuyên dụng của Network Agent được dành cho các ứng dụng chạy những hệ điều hành khác.

Network Agent Connector

Một chức năng của ứng dụng kết nối ứng dụng với Network Agent. Network Agent cho phép quản trị ứng dụng từ xa thông qua Kaspersky Security Center.

Nhóm quản trị

Một nhóm thiết bị chia sẻ chức năng chung và một bộ ứng dụng Kaspersky được cài đặt trên chúng. Các thiết bị được ghép nhóm để chúng có thể được quản lý một cách tiện lợi như một đơn vị duy nhất. Một nhóm có thể bao gồm các nhóm khác. Bạn có thể tạo các chính sách nhóm và tác vụ nhóm cho mỗi ứng dụng được cài đặt trong nhóm này.

Phạm vi bảo vệ

Các đối tượng liên tục được quét bởi thành phần bảo vệ chống virus khi thành phần này đang chạy. Phạm vi bảo vệ của các thành phần khác nhau có các thuộc tính khác nhau.

Phạm vi quét

Các đối tượng được Kaspersky Endpoint Security quét khi thực hiện một tác vụ quét.

Phân tích Dấu hiệu

Một công nghệ phát hiện mối đe dọa sử dụng cơ sở dữ liệu Kaspersky Endpoint Security chứa mô tả về các mối đe dọa đã biết và các phương thức để loại trừ chúng. Chế độ bảo vệ sử dụng phân tích dấu hiệu cung cấp một cấp độ bảo mật tối thiểu chấp nhận được. Theo khuyến nghị của các chuyên gia Kaspersky, phương thức này luôn được bật.

Phân tích Suy nghiệm

Công nghệ này được phát triển để phát hiện các mối đe dọa không thể được phát hiện với phiên bản cơ sở dữ liệu ứng dụng hiện tại của Kaspersky. Nó có thể phát hiện các tập tin bị nhiễm một loại virus không xác định, hoặc một biến thể mới của một virus đã biết.

Portable File Manager

Đây là một ứng dụng cung cấp giao diện để làm việc với các tập tin mã hóa trên ổ đĩa di động khi chức năng mã hóa không khả dụng trên máy tính.

Sao lưu

Một kho lưu trữ đặc biệt cho các bản sao dự phòng của các tập tin được tạo trước khi thực hiện khử nhiễm hoặc xóa.

Tác vụ

Các chức năng được thực hiện bởi các ứng dụng Kaspersky dưới dạng các tác vụ, ví dụ: Bảo vệ tập tin trong thời gian thực, Quét toàn bộ thiết bị, Cập nhật cơ sở dữ liệu.

Tập nén

Một hoặc nhiều tập tin được đóng gói vào một tập tin nén duy nhất. Một ứng dụng chuyên biệt gọi là trình nén tập tin là cần thiết để đóng góp và mở gói dữ liệu.

Tập tin bị nhiễm

Một tập tin có chứa mã độc (phát hiện được mã của các phần mềm độc hại đã biết khi quét tập tin này). Kaspersky không khuyến khích việc sử dụng các tập tin đó, bởi chúng có thể lây nhiễm virus cho máy tính.

Tập tin bị nhiễm

Một tập tin mà, theo cấu trúc hoặc định dạng của nó, có thể được sử dụng bởi kẻ xâm nhập làm "vỏ bọc" lưu trữ và phát tán mã độc. Nhìn chung, đây là các tập tin thực thi với các phần mở rộng như .com, .exe, và .dll. Có nhiều khả năng lây nhiễm mã độc trong các tập tin này.

Tập tin có khả năng bị nhiễm

Một tập tin chứa mã đã sửa đổi của một virus đã biết hoặc mã giống với một virus, nhưng chưa được Kaspersky biết đến. Tập tin có khả năng bị nhiễm được phát hiện bằng Trình phân tích suy nghiệm.

Thông tin về mã của bên thứ ba

Thông tin về mã của bên thứ ba được chứa trong tập tin legal_notices.txt, trong thư mục cài đặt của ứng dụng.

Thông báo thương hiệu

Các thương hiệu được đăng ký và nhãn hiệu dịch vụ là tài sản của các chủ sở hữu tương ứng.

Adobe, Acrobat, và Shockwave là các thương hiệu hoặc thương hiệu được đăng ký của Adobe Systems, được thành lập ở Hoa Kỳ và/hoặc các nơi khác.

Mac và FireWire là các thương hiệu của Apple, Inc., được đăng ký ở Hoa Kỳ và các nơi khác.

AutoCAD là một thương hiệu hoặc thương hiệu được đăng ký của Autodesk, Inc. và/hoặc các chi nhánh/công ty con của họ ở Hoa Kỳ và các nơi khác.

Ký tự thương hiệu Bluetooth và logo này là tài sản của Bluetooth SIG, Inc.

Borland là một thương hiệu hoặc thương hiệu được đăng ký của Borland Software Corporation ở Hoa Kỳ và các nơi khác.

Citrix và Citrix Provisioning Services là các thương hiệu của Citrix Systems, Inc. và/hoặc các chi nhánh của họ, được đăng ký với văn phòng cấp bằng sáng chế ở Hoa Kỳ và các quốc gia khác.

dBase là một thương hiệu của dataBased Intelligence, Inc.

EMC và SecurID là các thương hiệu hoặc thương hiệu được đăng ký của EMC Corporation ở Hoa Kỳ và các nơi khác.

ICQ là một thương hiệu và/hoặc nhãn hiệu dịch vụ của ICQ LLC.

Intel và Pentium là các thương hiệu của Intel Corporation, được đăng ký ở Hoa Kỳ và các nơi khác.

Logitech là một thương hiệu có đăng ký hoặc thương hiệu của Logitech Company ở Hoa Kỳ và các nơi khác.

Mail.ru là một thương hiệu được đăng ký của Mail.Ru LLC.

Microsoft, Windows, Internet Explorer, Access, Excel, PowerPoint, Outlook, Outlook Express, Windows Server, Visual Basic, Visual FoxPro, BitLocker, LifeCam Cinema, PowerShell và Surface là các thương hiệu của Microsoft Corporation, được đăng ký ở Hoa Kỳ và các nơi khác.

Mozilla và Thunderbird là các thương hiệu của Mozilla Foundation.

Novell là một thương hiệu của Novell Inc., được đăng ký ở Hoa Kỳ và các nơi khác.

Java và JavaScript là các thương hiệu được đăng ký của Oracle Corporation và/hoặc các chi nhánh của họ.

SafeNet là thương hiệu được đăng ký của SafeNet, Inc.

UNIX là một thương hiệu được đăng ký ở Hoa Kỳ và các nơi khác và được sử dụng theo giấy phép từ X/Open Company Limited.